Weakest Preconditions for High-Level Programs (Long Version)

Annegret Habel[1], Karl-Heinz Pennemann[1], and Arend Rensink[2]

[1] University of Oldenburg, Germany**
{habel,pennemann}@informatik.uni-oldenburg.de
[2] University of Twente, Enschede, The Netherlands
rensink@cs.utwente.nl

Abstract In proof theory, a standard method for showing the correctness of a program w.r.t. given pre- and postconditions is to construct a weakest precondition and to show that the precondition implies the weakest precondition. In this paper, graph programs in the sense of Habel and Plump 2001 are extended to programs over high-level rules with application conditions, a formal definition of weakest preconditions for high-level programs in the sense of Dijkstra 1975 is given, and a construction of weakest preconditions is presented.

1 Introduction

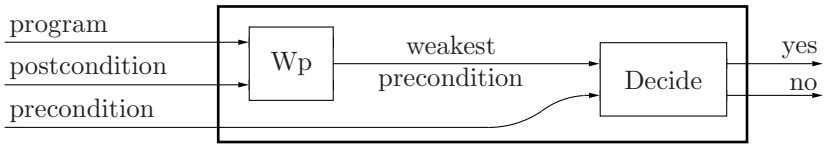
Graphs and related structures are associated with an accessible graphical representation. Transformation rules exploit this advantage, as they describe local change by relating a left- and a right-hand side. Nondeterministic choice, sequential composition and iteration give rise to rule-based programs [21].

Formal methods like verification with respect to a formal specification are important for the development of trustworthy systems. We use a graphical notion of conditions to specify valid objects as well as morphisms, e.g. matches for transformation rules. We distinguish the use of conditions by speaking of constraints in the first case, and application conditions for rules in the latter. Conditions seem to be adequate for describing requirements as well as for reasoning about the behavior of a system.

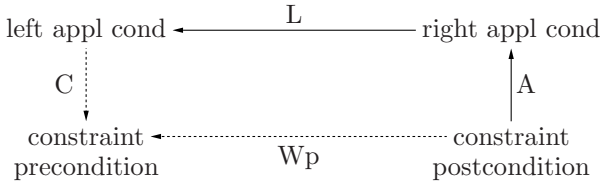
A well-known method for showing the correctness of a program with respect to a pre- and a postcondition (see e.g. [8,9]) is to construct a weakest precondition of the program relative to the postcondition and to prove that the precondition

** This work is supported by the German Research Foundation (DFG), grants GRK 1076/1 (Graduate School on Trustworthy Software Systems) and HA 2936/2 (Development of Correct Graph Transformation Systems).

implies the weakest precondition.



In this paper, we use the framework of weak adhesive HLR categories to construct weakest preconditions for high-level rules and programs, using two known transformations from constraints to right application conditions, and from right to left application conditions, and additionally, a new transformation from application conditions to constraints.



The paper is organized as follows. In Section 2, high-level conditions, rules and programs are defined and an access control for computer systems is introduced as a running example. In Section 3, two basic transformations of [18] are reviewed and, additionally, an essential transformation from application conditions into constraints is presented. In Section 4, weakest preconditions for high-level programs are formally defined and a transformation of programs and postconditions into weakest preconditions is given. In Section 5, related concepts and results are discussed. A conclusion including further work is given in Section 6. In Appendix A, the basic definitions of weak adhesive HLR categories together with their basic properties are collected. A formal definition of partial derivations within the execution of programs is given in Appenix B. Essential properties of weakest preconditions and general facts on implication and equivalence of conditions are given in Appendix C. Detailed proofs of some results are given in Appendix D, while Appenix E completes an example how to construct weakest preconditions. This report is a long version of [20].

2 Conditions and Programs

In this section, we review the definitions of conditions, rules, and programs for high-level structures, e.g. graphs. We use the framework of weak adhesive HLR categories introduced as combination of HLR systems and adhesive categories. The basic definitions and properties of weak adhesive HLR categories are given in Appendix A, whereas a detail introduction can be found in [15,17]. As a running example, we consider a simple graph transformation system consisting

of rules and programs. We demonstrate that programs are necessary extensions of rules for certain tasks and conditions can be used to describe a wide range of system properties, e.g. security properties.

Assumption. We assume that $\langle \mathcal{C}, \mathcal{M} \rangle$ is a weak adhesive HLR category with a category $\mathcal{C}$, a class $\mathcal{M}$ of monomorphisms, a $\mathcal{M}$-*initial* object, i.e., for every object G in $\mathcal{C}$, there exists an object I in $\mathcal{C}$ with unique morphism $I \to G$ in $\mathcal{M}$, binary coproducts and *epi-$\mathcal{M}$-factorization*, i.e. for every morphism there is an epi-mono-factorization with monomorphism in $\mathcal{M}$.

For illustration, we consider the category **Graph** of all directed, labeled graphs, which together with the class $\mathcal{M}$ of all injective graph morphisms constitutes a weak adhesive HLR category with binary coproducts and epi-$\mathcal{M}$-factorization and the empty graph $\emptyset$ as the $\mathcal{M}$-initial object.

Example 1 (access control graphs). In the following, we introduce state graphs of a simple access control for computer systems, which abstracts authentication and models user and session management in a simple way. We use this example solely for illustrative purposes. A more elaborated, role-based access control model is considered in [24]. The basic items of our model are users, sessions, logs, computer systems, and directed edges between those items. An edge between a user and a system represents that the user has the right to access the system, i.e. establish a session with the system. Every user node is connected with one log, while an edge from a log to the system represents a failed (logged) login attempt. Every session is connected to a user and a system. The direction of the latter edge differentiates between sessions that have been proposed (an outgoing edge from a session node to a system) and sessions that have been established (an incoming edge to a session node from a system). Self-loops may occur in graphs during the execution of programs to select certain elements, but not beyond. An example of an access control graph is given in Figure 1.

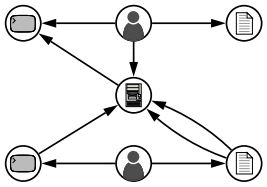


Figure 1. A state graph of the access control system

Conditions are nested constraints and application conditions in the sense of [18] generalizing the corresponding notions in [14] along the lines of [33].

Definition 1 (conditions). A *condition* over an object P is of the form $\exists a$ or $\exists(a, c)$, where $a\colon P \to C$ is a morphism and c is a condition over C. Moreover, Boolean formulas over conditions [over P] are conditions [over P]. Additionally,

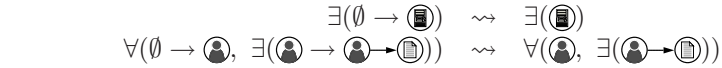
$\forall(a, c)$ abbreviates $\neg\exists(a, \neg c)$. A morphism $p\colon P \to G$ *satisfies* a condition $\exists a$ [$\exists(a, c)$] over P if there exists a morphism $q\colon C \to G$ in $\mathcal{M}$ with $q \circ a = p$ [satisfying c]. An object G *satisfies* a condition $\exists a$ [$\exists(a, c)$] if all morphisms $p\colon P \to G$ in $\mathcal{M}$ satisfy the condition. The satisfaction of conditions [over P] by objects [by morphisms with domain P] is extended onto Boolean conditions [over P] in the usual way. We write $p \models c$ [$G \models c$] to denote that morphism p [object G] satisfies c. Two conditions c and c' over P are *equivalent* on objects, denoted by $c \equiv c'$, if, for all objects G, $G \models c$ if and only if $G \models c'$.

We allow infinite conjunctions and disjunctions of conditions. In the context of objects, conditions are also called *constraints*, in the context of rules, they are called *application conditions*. As the required morphisms of the semantics are to be in $\mathcal{M}$, we sometimes speak of $\mathcal{M}$-satisfiability as opposed to $\mathcal{A}$-satisfiability, where $\mathcal{A}$ is the class of all morphisms (see [19]).

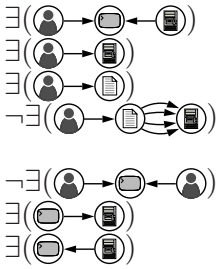
In the following we introduce a short notation for conditions, which can be used for application conditions over some rule-side L and for constraints over the $\mathcal{M}$-initial object I

Notation. For a morphism $a\colon P \to C$ in a condition, we just depict C, if P can be unambiguously inferred, i.e. for conditions over some left- or right-hand side and for constraints over the $\mathcal{M}$-initial object I. Note, that for every constraint over P, there is an equivalent constraint over I, i.e. $d \equiv \forall(I \to P, d)$, for $d = \exists a$ or $\exists(a, c)$.

Example 2 (short notation). The notation can be seen as a consequent generalization of the known shortcut $\exists C$. Consider the following graph constraints "There is a system node" and "Every user is associated with a log node" together with their short notations:



Example 3 (access control conditions). Consider the access control graphs introduced in Example 1. Conditions allow to formulate statements on the graphs of the access control and can be combined to form more complex statements. The following conditions are over the empty graph:



A user is logged into a system.
A user has an access right to a system.
A user is connected with a log.
There are not more than three failed, logged login attempts for any system and any user.
No two users are sharing a session.
A session is proposed.
A session is established.

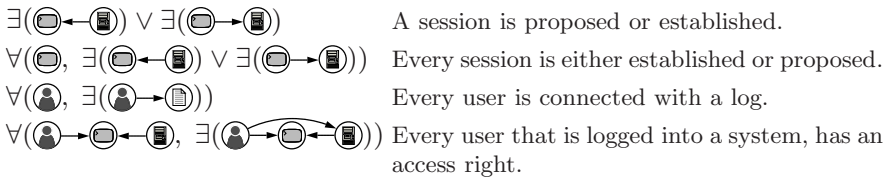


Figure 2. Conditions on access control graphs

We consider rules with application conditions [14,18]. Examples and pointers to the literature can be found in [12,7].

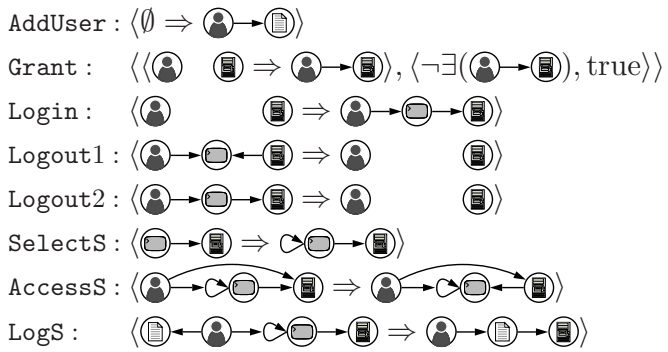
Definition 2 (rules). A *plain rule* $p = \langle L \leftarrow K \rightarrow R \rangle$ consists of two morphisms in $\mathcal{M}$ with a common domain K. L is called the left-hand side, R the right-hand side, and K the interface. An *application condition* $\mathrm{ac} = \langle \mathrm{ac}_L, \mathrm{ac}_R \rangle$ for p consists of two application conditions over L and R, respectively. A *rule* $\hat{p} = \langle p, \mathrm{ac} \rangle$ consists of a plain rule p and an application condition ac for p.

$$\begin{array}{ccccc} L & \longleftarrow & K & \longrightarrow & R \\ {\scriptstyle m}\downarrow & (1) & \downarrow & (2) & \downarrow{\scriptstyle m^*} \\ G & \longleftarrow & D & \longrightarrow & H \end{array}$$

Given a plain rule p and a morphism $K \rightarrow D$, a *direct derivation* consists of two pushouts (1) and (2). We write $G \Rightarrow_{p,m,m^*} H$, $G \Rightarrow_p H$, or short $G \Rightarrow H$ and say that m is the *match* and m^* is the *comatch* of p in H. Given a rule $\hat{p} = \langle p, \mathrm{ac} \rangle$ and a morphism $K \rightarrow D$, there is a *direct derivation* $G \Rightarrow_{\hat{p},m,m^*} H$ if $G \Rightarrow_{p,m,m^*} H$, $m \models \mathrm{ac}_L$, and $m^* \models \mathrm{ac}_R$. Let $\mathcal{A}$ be the class of all morphisms in $\mathcal{C}$. We distinguish between $\mathcal{A}$*-matching*, i.e. the general case, and $\mathcal{M}$*-matching*, i.e. if the match and the comatch are required to be in $\mathcal{M}$.

Notation. For the category **Graph**, we write $\langle L \Rightarrow R \rangle$ to abbreviate the rule $\langle L \leftarrow K \rightarrow R \rangle$, where K consists of all nodes common to L and R.

Example 4 (access control rules). Consider the access control graphs introduced in Example 1. The rules in Figure 3 are used to formalize the dynamic behavior of the access control system, i.e. are the basis of the access control programs.



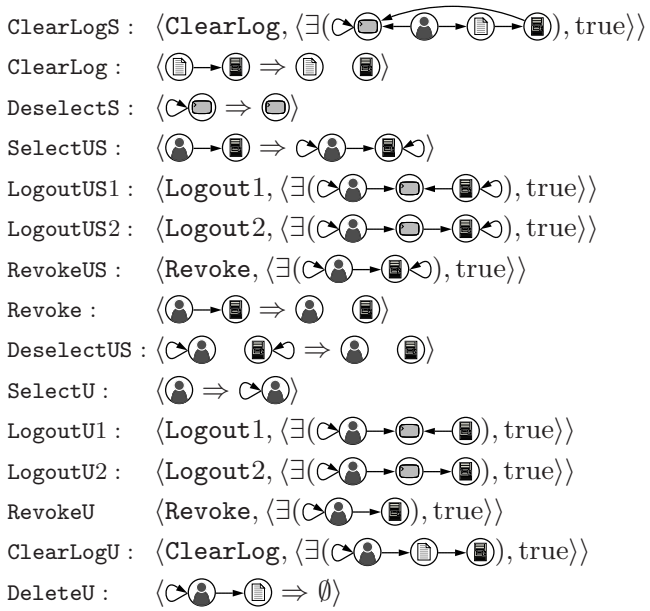


Figure 3. Rules of the access control system

Note, for every rule, every match is in $\mathcal{M}$. `AddUser` is a plain rule to introduce a user (and the associated log) to the system. `Grant` is a rule with application conditions: It grants a user the right to access a system, unless the user already has access. `Login` models a user proposing a session to a system, while `Logout1` and `Logout2` cancel an established or a proposed session, respectively. Rules with suffix `S`, `US` and `U` concern selected sessions (`S`), user and systems (`US`) and user (`U`) and are combined to programs in Figure 5. `SelectS` selects a session node by adding a self-loop. `AccessS` switches the status of the connection from proposed to established, if the user has an according access right. `LogS` will delete the session, and log the attempt, if the user is not authorized to connect. `ClearLogS` will remove one log entry of the session's user's log, if the connection is established. `DeselectS` deselects a session node by removing a self-loop. `SelectUS` selects a user and a system (with an access right). `LogoutUS` cancels a session of that user to that system. `RevokeUS` will remove an access right of the user to the system. `DeselectUS` deselects the user and the session. `SelectU` selects a user to delete by adding a self-loop. `LogoutU` cancels a session of a selected user. `RevokeU` removes an access right of a selected user. `DeleteU` deletes a selected user together with his/her log node, if no edges are adjacent to the nodes.

We generalize the notions of programs on linear structures [8,9] and graph programs [21,30]) to high-level programs on rules.

Definition 3 (programs). *(High-level) Programs* are inductively defined:

(1) `Skip` and every rule p are programs.
(2) Every finite set $\mathcal{S}$ of programs is a program.
(3) Given programs P and Q, then $(P;Q)$, P^* and $P\!\downarrow$ are programs.

The *semantics* of a program P is a binary relation $[\![P]\!] \subseteq \mathcal{C} \times \mathcal{C}$ on objects which is inductively defined as follows:

(1) $[\![\texttt{Skip}]\!] = \{\langle G, G\rangle \mid G \in \mathcal{C}\}$ and for every rule p, $[\![p]\!] = \{\langle G, H\rangle \mid G \Rightarrow_p H\}$.
(2) For a finite set $\mathcal{S}$ of programs, $[\![\mathcal{S}]\!] = \cup_{P\in\mathcal{S}}[\![P]\!]$.
(3) For programs P and Q, $[\![(P;Q)]\!] = [\![Q]\!] \circ [\![P]\!]$, $[\![P^*]\!] = [\![P]\!]^*$ and

$$[\![P\!\downarrow]\!] = \{\langle G, H\rangle \in [\![P]\!]^* \mid \neg\exists M.\ \langle H, M\rangle \in [\![P]\!]\}.$$

Programs according to (1) are *elementary*; a program according (2) describes the *nondeterministic choice* of a program; a program $(P;Q)$ is the *sequential composition* of P and Q, P^* is the *reflexive, transitive closure* of P, and $P\!\downarrow$ is the *iteration* of P as long as possible. Programs of the form $(P;(Q;R))$ and $((P;Q);R)$ are considered as equal; by convention, both can be written as $P;Q;R$.

Example 5 (access control programs). Consider the access control graphs in Example 1. The dynamic part of the control system `Control`* is the reflexive, transitive closure of the programs `Control` = {`AddUser`, `Grant`, `Login`, `Logout`, `ProcessLogin`, `Revoke`, `DeleteUser`}, depicted in Figure 4 and Figure 5, respectively. `Logout` cancels a session (established or proposed). `ProcessLogin` models

```
Logout       = {Logout1, Logout2}
ProcessLogin = SelectS; AccessS↓; LogS↓; ClearLogS↓; DeselectS↓
Revoke       = SelectUS; LogoutUS↓; RevokeUS; DeselectUS
LogoutUS     = {LogoutUS1, LogoutUS2}
DeleteUser   = SelectU; LogoutU↓; RevokeU↓; ClearLogU↓; DeleteU
LogoutU      = {LogoutU1, LogoutU2}
```

Figure 4. Programs of the access control system

the reaction of a system towards a session proposal, which, dependent on the user's right, leads to an established session and the clearing of the user's log of failed attempts, or the denial and removal of that session and the logging of the failed attempt. `Revoke` removes a user's right to access a system, but not before closing the user's sessions to that system. Finally, `DeleteUser` is a program to delete a user and his/her associated log by canceling the user's sessions, by removing the user's access rights and by clearing the user's log.

Note, that there is no way to model certain actions like `DeleteUser` by a single rule, as a user, in principle, may have an arbitrary number of sessions or log entries. However, user deletion should be a transaction always applicable for every user.

Remark 1. The definition of programs generalizes the one in [21]: We consider a weak adhesive HLR category instead of the category of all directed, labeled graphs. The programs are based on rules with application conditions instead of plain rules. Moreover, we allow an explicit demonic nondeterministic choice of programs. Every program in the sense of [21] is a program in our sense. By the computational completeness result in [21], our language is expressively equivalent to the one in [21] and closely related to programs on linear structures in the sense of [8,9].

Definition 4 (termination). A program P applied to an input object G *terminates* properly, if $\mathrm{PDer}(P, G)$ is finite, i.e. $\exists k \in \mathbb{N}.\ |\mathrm{PDer}(P, G)| \leq k$, where $\mathrm{PDer}(P, G)$ denotes the set of all partial derivations within the execution of a program P, starting with G (see Definition of partial derivations, Appendix B).

Remark 2. Execution of high-level programs requires backtracking, therefore the above definition of termination is more suitable than the classical one, i.e. the nonexistence of infinite derivations. This may be seen as follows: An infinite derivation implies infinitely many partial derivations. The other direction holds only if the number of matches is finite. By the uniqueness of pushouts, $\mathrm{PDer}(p, G)$ is finite and there cannot be infinitely many derivations of finite length for any program P.

3 Basic Transformations of Conditions

In the following, we recall two known transformations from constraints to application conditions and from right- to left application conditions [23,14,18] and present a new transformation from application conditions to constraints. Combining these basic transformations, we obtain a transformation from a postcondition over the rule to a precondition. First, there is a transformation from constraints to application conditions such that a morphism satisfies the application condition if and only if the codomain satisfies the constraint.

Theorem 1 (transformation of constraints into application conditions). *There is a transformation* A *such that, for every constraint* c *and every rule* $p = \langle L \leftarrow K \rightarrow R \rangle$*, and all morphisms* $m^*\colon R \rightarrow H$*,* $m^* \models \mathrm{A}(p, c) \Leftrightarrow H \models c$*.*

Second, there is a transformation from right to left application conditions such that a comatch satisfies an application condition if and only if the match satisfies the transformed application condition.

Theorem 2 (transformation of application conditions). *There is a transformation* L *such that, for every rule* p*, every right application condition* ac *for* p*, and all direct derivations* $G \Rightarrow_{p,m,m^*} H$*,* $m \models \mathrm{L}(p, \mathrm{ac}) \Leftrightarrow m^* \models \mathrm{ac}$*.*

We consider a transformation of application conditions to constraints, which correspond to the universal closure of application conditions. For $\mathcal{A}$-matching

however, the closure is over arbitrary morphisms and does not fit to the notion of $\mathcal{M}$-satisfiability. This is why a part of the application condition has to be transformed accordingly.

Theorem 3 (transformation of application conditions into constraints). *For weak adhesive HLR categories with $\mathcal{M}$-initial object, there is a transformation* C *such that, for every application condition* ac *over L and for all objects G,*

$$G \models \mathrm{C}(\mathrm{ac}) \Leftrightarrow \forall m\colon L \to G.\ m \models \mathrm{ac}$$

Construction. Define $\mathrm{C}(\mathrm{ac}) = \bigwedge_{e \in E}\ \forall(e \circ i,\ \mathrm{C}_e(\mathrm{ac}))$ where the junction ranges over all epimorphisms $e\colon L \to L'$ and $i\colon I \to L$ is the unique morphism from the $\mathcal{M}$-initial object to L. The transformation C_e is defined inductively on the structure of the conditions: $\mathrm{C}_e(\exists a) = \exists a'$ and $\mathrm{C}_e(\exists(a, c)) = \exists(a', c)$ if $a = a' \circ e$ is some epi-$\mathcal{M}$-factorization of a and $\mathrm{C}_e(\exists a) = \mathrm{C}_e(\exists(a, c)) = \mathrm{false}$ if there is no epi-$\mathcal{M}$-factorization of a with epimorphism e. For Boolean conditions, the transformation C_e is extended in the usual way.

Example 6. The application condition $\mathrm{ac} = \neg\exists(\,\to\,) \wedge \neg\exists(\,\leftarrow\,) \wedge \neg\exists(\,\circlearrowleft\,)$ over $\;\;$ expresses that there is no edge between two given session nodes.

$$\begin{aligned}
\mathrm{C}(\mathrm{ac}) = \quad & \forall(\;\;,\ \mathrm{C}_{\mathrm{id}}(\mathrm{ac})) \wedge \forall(\;,\ \mathrm{C}_e(\mathrm{ac})) \\
= \quad & \forall(\;\;,\ \neg\mathrm{C}_{\mathrm{id}}(\exists(\,\to\,)) \wedge \neg\mathrm{C}_{\mathrm{id}}(\exists(\,\leftarrow\,)) \wedge \neg\mathrm{C}_{\mathrm{id}}(\exists(\,\circlearrowleft\,))) \\
\wedge\ & \forall(\;,\quad \neg\mathrm{C}_e(\exists(\,\to\,)) \wedge \neg\mathrm{C}_e(\exists(\,\leftarrow\,)) \wedge \neg\mathrm{C}_e(\exists(\,\circlearrowleft\,))) \\
= \quad & \forall(\;\;,\ \mathrm{ac}) \wedge \forall(\;,\ \neg\mathrm{false} \wedge \neg\mathrm{false} \wedge \neg\exists(\,\circlearrowleft\,)) \\
\equiv \quad & \forall(\;\;,\ \neg\exists(\,\to\,) \wedge \neg\exists(\,\leftarrow\,) \wedge \mathrm{true}) \wedge \forall(\;,\ \mathrm{true} \wedge \neg\exists(\,\circlearrowleft\,)) \\
\equiv \quad & \forall(\;\;,\ \neg\exists(\,\to\,) \wedge \neg\exists(\,\leftarrow\,)) \wedge \forall(\;,\ \neg\exists(\,\circlearrowleft\,))
\end{aligned}$$

with $\mathrm{id}\colon \;\; \to \;\;$ and $e\colon \;\; \to \;$.

Proof. In [19] is shown: For all $m'\colon L' \to G$ in $\mathcal{M}$ and all epimorphisms $e\colon L \to L'$,

$$m' \models \mathrm{C}_e(\mathrm{ac}') \quad \Leftrightarrow \quad m' \circ e \models \mathrm{ac}' \qquad (*)$$

We show: $\forall m\colon L \to G,\ m \models \mathrm{ac}$ if and only if $G \models \mathrm{C}(\mathrm{ac})$. "Only if". Assume $\forall m\colon L \to G,\ m \models \mathrm{ac}$. For $G \models \mathrm{C}(\mathrm{ac})$ to hold, G has to satisfy $\mathrm{C}_e(\mathrm{ac})$ for all epimorphisms $e\colon L \to L'$, i.e. for all epimorphisms $e\colon L \to L'$ and all morphisms $m'\colon L' \to G$ in $\mathcal{M}$ holds $m' \models \mathrm{C}_e(\mathrm{ac})$. Given such morphisms e and m', define $m = m' \circ e$. By assumption, $m \models \mathrm{ac}$, and by $(*)$ we have $m' \models \mathrm{C}_e(\mathrm{ac})$, hence $G \models \mathrm{C}(\mathrm{ac})$. "If". Assume $G \models \mathrm{C}(\mathrm{ac})$, i.e. G satisfies $\mathrm{C}_e(\mathrm{ac})$ for all epimorphisms $e\colon L \to L'$, i.e. for all epimorphisms $e\colon L \to L'$ and all morphisms $m'\colon L' \to G$ in $\mathcal{M}$ holds $m' \models \mathrm{C}_e(\mathrm{ac})$. Given an arbitrary morphism $m\colon L \to G$, consider the epi-$\mathcal{M}$-factorization $m' \circ e$. By assumption, $m' \models \mathrm{C}_e(\mathrm{ac})$, and by $(*)$ we have $m \models \mathrm{ac}$.

Remark 3. The uniqueness of epi-$\mathcal{M}$-factorizations (up to isomorphism) follows immediately from the uniqueness of epi-mono-factorizations, as every $\mathcal{M}$-morphism is a monomorphism.

Remark 4. For weak adhesive HLR categories with $\mathcal{M}$-initial object and $\mathcal{M}$-matching, there is a simplified transformation C such that, for every application condition ac over L and for all objects G, $G \models \mathrm{C}(\mathrm{ac}) \Leftrightarrow \forall m\colon L \to G \in \mathcal{M}.\ m \models \mathrm{ac}$.

For an application condition ac over L and $i\colon I \to L$, let $\mathrm{C}(\mathrm{ac}) = \forall(i, \mathrm{ac})$. For all $\mathcal{M}$-morphisms $m\colon L \to G$, $m \models \mathrm{ac}$ iff there exists an $\mathcal{M}$-morphism $p\colon I \to G$ such that for all $\mathcal{M}$-morphisms $m\colon L \to G$ holds $m \models \mathrm{ac}$ iff there exists an $\mathcal{M}$-morphism $p\colon I \to G$ such that for all $\mathcal{M}$-morphisms $m\colon L \to G$ with $p = m \circ i$ holds $m \models \mathrm{ac}$ iff $G \models \forall(i, \mathrm{ac})$ (Definition 1).

Finally, the applicability of a rule can be expressed by a left application condition for the matching morphism.

Theorem 4 (applicability of a rule). *There is a transformation* Def *from rules into application conditions such that, for every rule p and every morphism $m\colon L \to G$,*

$$m \models \mathrm{Def}(p) \Leftrightarrow \exists H.G \Rightarrow_{p,m,m^*} H.$$

Construction. For a rule $p = \langle q, \mathrm{ac}\rangle$, let $\mathrm{Def}(p) = \mathrm{Appl}(q) \wedge \mathrm{ac}_L \wedge \mathrm{L}(p, \mathrm{ac}_R)$, where, for a rule $q = \langle L \xleftarrow{l} K \xrightarrow{r} R\rangle$, $\mathrm{Appl}(q) = \wedge_{a \in A} \neg\exists a$ and the index set A ranges over all morphisms $a\colon L \to L'$ such that the pair $\langle l, a\rangle$ has no pushout complement and there is no decomposition $a = a'' \circ a'$ of a with proper morphism a'' in $\mathcal{M}$ (a'' not an isomorphism) such that $\langle l, a'\rangle$ has no pushout complement.

Example 7. An example of Appl is given below for $\texttt{DeleteSys} = \langle$  $\leftarrow \emptyset \rightarrow \emptyset\rangle$. Intuitively, the application of `DeleteSys` requires the absence of additional edges adjacent to the system node. Therefore, `DeleteSys` may only be the last step in program deleting a system node. Appl(`DeleteSys`) is a condition over .

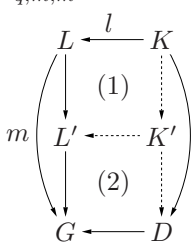
$\mathrm{Appl}(\texttt{DeleteSys}) =$ 

Proof. For plain rules, we show that, for every morphism $m\colon L \to G$,

$$m \models \mathrm{Appl}(q) \Leftrightarrow \exists H.G \Rightarrow_{q,m,m^*} H.$$

"Only if" Let $m \models \mathrm{Appl}(q)$. Assume there is no direct derivation $G \Rightarrow_{q,m,m^*} H$. Then the pair $\langle l, m\rangle$ has no pushout complement and there is a morphism $a\colon L \to L'$ such that $\langle l, a\rangle$ has no pushout complement and $m \models \exists a$. Then $m \not\models \mathrm{Appl}(q)$. A contradiction. Consequently, there is a direct derivation $G \Rightarrow_{q,m,m^*} H$.

"If" Let $G \Rightarrow_{q,m,m^*} H$. Then, for every morphism $a\colon L \to L'$, $m \models \exists a$ iff there is some $m'\colon L' \to G$ in $\mathcal{M}$ such that $m' \circ a = m$. By the pushout-pullback decomposition, the pushout has a decomposition into two pushouts (1) and (2) and, in particular, $\langle l, a\rangle$ has a pushout complement. Consequently, for every morphism $a \in A$, $m \models \neg\exists a$, i.e. $m \models \mathrm{Appl}(q)$.



By the definition of Def and $\models$, Theorem 4, the statement above, and the definition of $\Rightarrow$, for every morphism $m\colon L \to G$, $m \models \mathrm{Def}(p)$ iff $m \models \mathrm{Appl}(q) \wedge m \models \mathrm{ac}_L \wedge m \models \mathrm{L}(p, \mathrm{ac}_R)$ iff $\exists H.G \Rightarrow_{q,m,m^*} H \wedge m \models \mathrm{ac}_L \wedge m^* \models \mathrm{ac}_R$ iff $\exists H.G \Rightarrow_{p,m,m^*} H$. This completes the proof.

4 Weakest Preconditions

In the following, we define weakest preconditions for high-level programs similar to the ones for Dijkstra's guarded commands in [8,9], show how to construct weakest preconditions for high-level programs and demonstrate the use of weakest preconditions to reduce problems on programs, e.g. the invariance of conditions, onto tautology problems of conditions.

Definition 5 (weakest preconditions). For a program P relative to a condition d we define: A condition c is a *precondition*, if for all objects G satisfying c,

(1) $\langle G, H\rangle \in [\![P]\!]$ implies $H \models d$ for all H,
(2) $\langle G, H\rangle \in [\![P]\!]$ for some H, and
(3) P terminates for G.

A condition c is a *liberal* precondition, if for all objects $G \models c$ at least (1) is satisfied, and a *termination* precondition, if for all objects $G \models c$ at least (1) and (3) is satisfied. A precondition c is a *weakest precondition*, denoted by $\mathrm{wp}(P, d)$, if all other preconditions c' of P relative to d imply c. *Weakest liberal* and *weakest termination preconditions*, denoted by $\mathrm{wlp}(P, d)$ and $\mathrm{wtp}(P, d)$, respectively, are defined analogously.

Example 8 (weakest precondition). Consider the access control rules in Example 4. A weakest precondition for the rule `SelectU`: $\langle$  $\Rightarrow$  $\rangle$ and the postcondition $\neg\exists($   $)$ is $\neg\exists($$)$.

The following fact points out a simple proof scheme for weakest preconditions.

Fact 1 (weakest preconditions). A condition c is a weakest precondition if, for all objects G, $G \models c$ if and only if properties (1)-(3) are satisfied.

Proof. By definition, c is a precondition. For any other precondition c', for every object G, $G \models c'$ implies properties (1)-(3) are satisfied (c' is a precondition), which implies $G \models c$, hence c' implies c.

For the construction of weakest preconditions, we make use of the fact that $\mathrm{wp}(P, d)$ is a conjunction of three properties and treat properties (1) and (3), and property (2) separately. We observe property (2) is equivalent to the negation of property (1) for $d = \neg\mathrm{true}$, hence we state:

Fact 2 (existence of results). $G \models \neg\mathrm{wlp}(P, \mathrm{false}) \Leftrightarrow$ property (2) is satisfied.

Proof. There is an object H such that $\langle G, H\rangle \in [\![P]\!]$, if and only if there is an object H such that $\langle G, H\rangle \in [\![P]\!]$ and $H \models \text{true}$, if and only if not for all objects H holds not ($\langle G, H\rangle \in [\![P]\!]$ and $H \models \text{true}$), if and only if not for all objects H holds not $\langle G, H\rangle \in [\![P]\!]$ or $H \not\models \text{true}$, if and only if not for all objects H holds $\langle G, H\rangle \in [\![P]\!]$ implies $H \models \text{false}$.

Theorem 5 (weakest liberal preconditions). *There is a transformation* Wlp*, such that for every program P and every condition d,* $\mathrm{Wlp}(P, d)$ *is a weakest liberal precondition of P relative to d.*

Construction. The transformation is defined inductively over the structure of programs. For any rule p, any set $\mathcal{S}$ of programs and programs P, Q,

$$\begin{array}{ll}
\mathrm{Wlp}(p, d) & = \mathrm{C}(\mathrm{Def}(p) \Rightarrow \mathrm{L}(p, \mathrm{A}(p, d))) \\
\mathrm{Wlp}(\texttt{Skip}, d) & = d \\
\mathrm{Wlp}(\mathcal{S}, d) & = \bigwedge_{P \in \mathcal{S}} \mathrm{Wlp}(P, d) \\
\mathrm{Wlp}((P; Q), d) & = \mathrm{Wlp}(P, \mathrm{Wlp}(Q, d)) \\
\mathrm{Wlp}(P^*, d) & = \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, d) \\
\mathrm{Wlp}(P{\downarrow}, d) & = \mathrm{Wlp}(P^*, \mathrm{Wlp}(P, \text{false}) \Rightarrow d)
\end{array}$$

where for $i \geq 0$, P^i is inductively defined by $\texttt{Skip}$ for $i = 0$ and by $P^{i+1} = (P^i; P)$.

Proof. We show $\mathrm{Wlp}(P, d) \equiv \mathrm{wlp}(P, d)$ by induction over the structure of programs. For elementary programs consisting of a single rule p, we have: For all objects G,

$$\begin{array}{lll}
& G \models \mathrm{Wlp}(p, d) & \\
\Leftrightarrow & G \models \mathrm{C}(\mathrm{Def}(p) \Rightarrow \mathrm{L}(p, \mathrm{A}(p, d))) & \text{(Def. Wlp)} \\
\Leftrightarrow & \forall L \overset{m}{\to} G.\ m \models (\mathrm{Def}(p) \Rightarrow \mathrm{L}(p, \mathrm{A}(p, d))) & \text{(Thm. 3)} \\
\Leftrightarrow & \forall L \overset{m}{\to} G.\ m \models \mathrm{Def}(p) \Rightarrow m \models \mathrm{L}(p, \mathrm{A}(p, d)) & \text{(Def. } \models\text{)} \\
\Leftrightarrow & \forall L \overset{m}{\to} G, R \overset{m^*}{\to} H.\ m \models \mathrm{Def}(p) \Rightarrow m^* \models \mathrm{A}(p, d) & \text{(Thm. 2)} \\
\Leftrightarrow & \forall L \overset{m}{\to} G, R \overset{m^*}{\to} H.\ (G \Rightarrow_{p,m,m^*} H) \Rightarrow H \models d & \text{(Thms. 4 \& 1)} \\
\Leftrightarrow & \forall H.\ \langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d & \text{(Def. } [\![p]\!]\text{)} \\
\Leftrightarrow & G \models \mathrm{wlp}(p, d) & \text{(Def. wlp)}
\end{array}$$

Thus, $\mathrm{Wlp}(p, d)$ is a weakest liberal precondition of p relative to d. For composed programs, the statement follows by structural induction (see Appendix D).

Assumption. We assume that $\langle \mathcal{C}, \mathcal{M}\rangle$ is a weak adhesive HLR category with finite number of matches, i.e. for every morphism $l\colon K \to L$ in $\mathcal{M}$ and every object G, there exist only a finite number of morphisms $m\colon L \to G$ s.t. $\langle l, m\rangle$ has a pushout complement.

Theorem 6 (weakest preconditions). *For weak adhesive HLR categories with finite number of matches, there are transformations* Wtp *and* Wp *such that for every program P and every condition d,* $\mathrm{Wtp}(P, d)$ *is a weakest termination precondition and* $\mathrm{Wp}(P, d)$ *is a weakest precondition of P relative to d.*

Construction. For any program P, $\mathrm{Wp}(P,d) = \mathrm{Wtp}(P,d) \wedge \neg\mathrm{Wlp}(P,\mathrm{false})$, where Wtp is inductively defined for any rule p, any set $\mathcal{S}$ of programs and programs P, Q as follows:

$$\begin{array}{ll}
\mathrm{Wtp}(p,d) & = \mathrm{Wlp}(p,d) \\
\mathrm{Wtp}(\texttt{Skip},d) & = d \\
\mathrm{Wtp}(\mathcal{S},d) & = \bigwedge_{P\in\mathcal{S}} \mathrm{Wtp}(P,d) \\
\mathrm{Wtp}((P;Q),d) & = \mathrm{Wtp}(P,\mathrm{Wtp}(Q,d)) \\
\mathrm{Wtp}(P^*,d) & = \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, d \wedge \mathrm{Wtp}(P,\mathrm{true})) \wedge \bigvee_{k=0}^{\infty} \mathrm{Wlp}(P^{k+1},\mathrm{false}) \\
\mathrm{Wtp}(P{\downarrow},d) & = \mathrm{Wtp}(P^*, \mathrm{Wlp}(P,\mathrm{false}) \Rightarrow d)
\end{array}$$

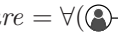
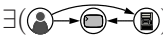
where for $i \geq 0$, P^i is inductively defined by `Skip` for $i = 0$ and by $P^{i+1} = (P^i; P)$.

Proof. We show $\mathrm{Wtp}(P,d) \equiv \mathrm{wtp}(P,d)$, and $\mathrm{Wp}(P,d) \equiv \mathrm{wp}(P,d)$. The first proof is done by induction over the structure of programs. For elementary programs consisting of a single rule p, we have: For every object G, $G \models \mathrm{Wtp}(p,d)$ if and only if $G \models \mathrm{Wlp}(p,d)$, as every rule application terminates by the finiteness assumption and wtp reduces to wlp for single rules p. For composed programs, the statement follows by structural induction (see Appendix D).

For Wp, we now show for every program P, $\mathrm{Wp}(P,d) \equiv \mathrm{wp}(P,d)$: $\mathrm{Wp}(P,d)$ is defined as $\neg\mathrm{Wlp}(P,\mathrm{false}) \wedge \mathrm{Wtp}(P,d)$, which is, by the first two equations, equivalent to $\neg\mathrm{wlp}(P,\mathrm{false}) \wedge \mathrm{wtp}(P,d)$, which is equivalent to $\mathrm{wp}(P,d)$ (see Fact 4.(4), Appendix D).

Example 9 (access control system). Consider the access control for computer systems, presented in Examples 1-5. For the system, one might want to ensure the validity of certain properties, e.g.:

(1) Always, every user logged into a system has an access right to the system: *secure* implies wlp(`Control`, *secure*), where

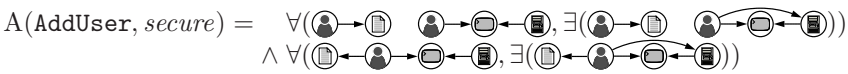
$$\mathit{secure} = \forall(\text{  }, \exists(\text{  })).$$

(2) Every user can always be deleted: $\exists(\text{  })$ implies $\mathrm{wp}(\texttt{DeleteUser},\mathrm{true})$

(3) Every user can always have his access right to a system revoked: $\exists(\text{  })$ implies $\mathrm{wp}(\texttt{Revoke},\mathrm{true})$

By calculating weakest [liberal] preconditions, the problem to decide these properties can be reduced onto the tautology problem for conditions. For a program P, the meaning of *secure* implies wlp(P, *secure*) can be seen as follows: The constraint *secure* is invariant for P, i.e., given an input state satisfying *secure*, any result of P will satisfy *secure*. According to the definition of Wlp, we would have to show *secure* implies $\mathrm{Wlp}(P,\mathit{secure})$ for every program $P \in$ `Control`.

For the program `AddUser`, we prove *secure* implies Wlp(`AddUser`, *secure*):

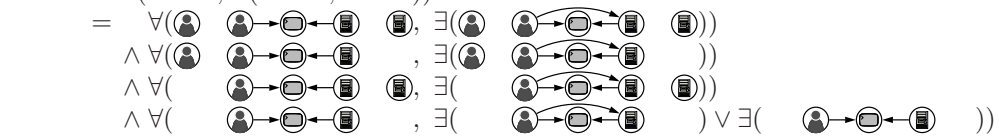
$\mathrm{A}(\texttt{AddUser}, \mathit{secure}) =$ 

$\mathrm{L}(\texttt{AddUser}, \mathrm{A}(\texttt{AddUser}, \mathit{secure})) =$ 

$$\begin{aligned}\mathrm{Wlp}(\texttt{AddUser}, \mathit{secure}) &= \mathrm{C}(\mathrm{Def}(\texttt{AddUser}) \Rightarrow \mathrm{L}(\texttt{AddUser}, \mathrm{A}(\texttt{AddUser}, \mathit{secure})))\\ &= \mathrm{C}((\mathrm{Appl}(\texttt{AddUser}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathit{secure})\\ &\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathit{secure}) \equiv \mathrm{C}(\mathit{secure})\\ &= \forall(\emptyset, \mathit{secure})\\ &\equiv \mathit{secure}\end{aligned}$$

where we use Fact 5.(2) for the second last step. The validity of the statement is no surprise as we could have argued that a newly added user cannot have an established session with a system, hence every application of `AddUser` preserves the satisfaction of *secure*. For the program `Grant`, *secure* implies Wlp(`Grant`, *secure*), even without the additional application condition.

$\mathrm{L}(\texttt{Grant}, \mathrm{A}(\texttt{Grant}, \mathit{secure}))$

$=$ 

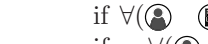
$\mathrm{Wlp}(\texttt{Grant}, \mathit{secure})$

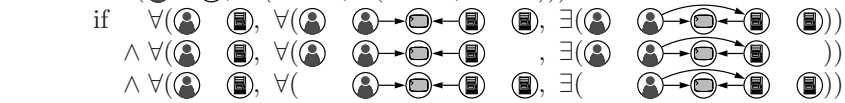
$= \mathrm{C}(\mathrm{Def}(\texttt{Grant}) \Rightarrow \mathrm{L}(\texttt{Grant}, \mathrm{A}(\texttt{Grant}, \mathit{secure})))$

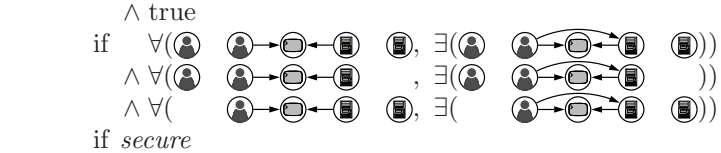
$= \mathrm{C}((\mathrm{Appl}(\texttt{Grant}) \wedge \neg\exists(\,\,) \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{Grant}, \mathrm{A}(\texttt{Grant}, \mathit{secure})))$

$\equiv \mathrm{C}(\neg\exists(\,\,) \Rightarrow \mathrm{L}(\texttt{Grant}, \mathrm{A}(\texttt{Grant}, \mathit{secure})))$

if $\mathrm{C}(\mathrm{L}(\texttt{Grant}, \mathrm{A}(\texttt{Grant}, \mathit{secure})))$

if 

if 

if 

if *secure*

where we use Fact 5.(1), 5.(2) and 5.(4) for the last three steps respectively (see Appendix C). The validity of the statement can be seen as follows: For a user and a system, `Grant` adds the corresponding access right. Apart from the left application condition, if there was already an established session from that user to that system, the precondition *secure* would have ensured the presence of a corresponding access right. The same holds for every other user and/or system.

This example is continued in Appendix E.

5 Related concepts

In this section we briefly review other work on using graph transformation for verification. Before we do so, however, we wish to point out one important global difference between this related work and the approach of this paper.

- The approach of this paper is based on the principle of *assertional reasoning*, and inherits both the advantage and the disadvantage of that principle. The advantage is that the approach is general where it can be made to apply, meaning that it provides a method to verify finite-state and infinite-state systems alike. The disadvantage is that finding invariants is hard and cannot be automated in general.
- Existing approaches are typically based on the principle of *model checking*, which essentially involves exhaustive exploration, either of the concrete states (which are often too numerous to cover completely) or on some level of abstraction (in which case the results become either unsound or incomplete). On the positive side, model checking is a push-button approach, meaning that it requires no human intervention.

In other words, there is a dividing line between the work in this paper and the related work reported below, which is parallel to the division between theorem proving and model checking in "mainstream" verification (see [22] for an early discussion). Since current wisdom holds that these approaches can actually be combined to join strengths (e.g., [6,28]), we expect that the same will turn out to hold in the context of graph transformation.

The first paper in which it was put forward that graph transformation systems can serve as a suitable specification formalism on the basis of which model checking can be performed was Varró [35]; this was followed up by [36] which describes a tool chain by which graph transformation systems are translated to Promela, and then model checked by SPIN. We pursued a similar approach independently in [31,32], though relying on dedicated (graph transformation-based) state space generation rather than an existing tool. The two strands were compared in [34]. Again independently, Dotti et al. [11,10] also describe a translation from a graph transformation-based specification formalism (which they call object-based graph grammars) to Promela.

Another model checking-related approach, based on the idea of McMillan unfoldings for Petri Nets (see [27]), has been pursued by Baldan, König et al. in, e.g., [3,2], and in combination with abstraction in [4,25]. The latter avoids the generation of complete (concrete) state spaces, at the price of being approximative, in other words, admitting either false positives (unsoundness) or false negatives (incompleteness) in the analysis. The (pure) model checking and abstraction-based techniques were briefly compared in [5].

Termination. In addition to the general verification methods discussed above, a lot of research has been carried out on more specific properties of graph grammars. Especially relevant in our context is the work on *termination* of graph

grammars. This is known to be undecidable in general (see [29]), but under special circumstances may be shown to hold; for instance, Ehrig et al. discuss such a special case for *model transformation* in [13].

6 Conclusion

This paper extends graph programs to programs over high-level rules with application conditions, and defines weakest preconditions over high-level programs similar to the ones for Dijkstra's guarded commands in [8,9]. It presents transformations from application conditions to constraints, which, combined with two known transformations over constraints and application conditions, can be used to construct weakest preconditions for high-level rules as well as programs.

A known proof technique for showing the correctness of a program with respect to a pre- and a postcondition is to construct a weakest precondition and to show that the precondition implies the weakest precondition. We demonstrate the applicability of this method on our access control for computer systems.

Further topics could be the followings.

(1) Consideration of strongest postconditions.
(2) Comparison of notions: A comparison of conditions – as considered in this paper – and first-order formulas on graphs and high-level structures.
(3) Generalization of notions: The generalization of conditions to capture monadic second order properties.
(4) An investigation of the tautology problem for conditions with the aim to find a suitable class of conditions, for which the problem is decidable.
(5) Implementation: A system for computing/approximating weakest preconditions and for deciding/semideciding correctness of program specifications [1].

References

1. K. Azab, A. Habel, K.-H. Pennemann, and C. Zuckschwerdt. ENFORCe: A system for ensuring formal correctness of high-level programs. In *Preliminary Proc. 3rd International Workshop on Graph Based Tools (GraBaTs'06)*, 2006. To appear.
2. P. Baldan, A. Corradini, and B. König. Verifying finite-state graph grammars. In *Concurrency Theory*, volume 3170 of *LNCS*, pages 83–98. Springer, 2004.
3. P. Baldan and B. König. Approximating the behaviour of graph transformation systems. In *Graph Transformations (ICGT'02)*, volume 2505 of *LNCS*, pages 14–29. Springer, 2002.
4. P. Baldan, B. König, and B. König. A logic for analyzing abstractions of graph transformation systems. In *Static Analysis Symposium (SAS)*, volume 2694 of *LNCS*, pages 255–272. Springer, 2003.
5. P. Baldan, B. König, and A. Rensink. Graph grammar verification through abstraction. In B. König, U. Montanari, and P. Gardner, editors, *Graph Transformations and Process Algebras for Modeling Distributed and Mobile Systems*, number 04241 in Dagstuhl Seminar Proceedings, 2005.

6. E. M. Clarke, A. Biere, R. Raimi, and Y. Zhu. Bounded model checking using satisfiability solving. *Formal Methods in System Design*, 19(1):7–34, 2001.
7. A. Corradini, U. Montanari, F. Rossi, H. Ehrig, R. Heckel, and M. Löwe. Algebraic approaches to graph transformation. In *Handbook of Graph Grammars and Computing by Graph Trans.*, volume 1, pages 163–245. World Scientific, 1997.
8. E. W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976.
9. E. W. Dijkstra and C. S. Scholten. *Predicate Calculus and Program Semantics*. Springer, 1989.
10. O. M. dos Santos, F. L. Dotti, and L. Ribeiro. Verifying object-based graph grammars. *ENTCS*, 109:125–136, 2004.
11. F. L. Dotti, L. Foss, L. Ribeiro, and O. M. dos Santos. Verification of distributed object-based systems. In *Formal Methods for Open Object-Based Distributed Systems (FMOODS)*, volume 2884 of *LNCS*, pages 261–275. Springer, 2003.
12. H. Ehrig. Introduction to the algebraic theory of graph grammars. In *Graph-Grammars and Their Application to Computer Science and Biology*, volume 73 of *LNCS*, pages 1–69. Springer, 1979.
13. H. Ehrig, K. Ehrig, J. De Lara, G. Taentzer, D. Varró, and S. Varró-Gyapay. Termination criteria for model transformation. In *Proc. Fundamental Approaches to Software Engineering*, volume 2984 of *LNCS*, pages 214–228. Springer, 2005.
14. H. Ehrig, K. Ehrig, A. Habel, and K.-H. Pennemann. Theory of constraints and application conditions: From graphs to high-level structures. *Fundamenta Informaticae*, 2006. To appear.
15. H. Ehrig, K. Ehrig, U. Prange, and G. Taentzer. *Fundamentals of Algebraic Graph Transformation*. EATCS Monographs of Theoretical Computer Science. Springer-Verlag, Berlin, 2006.
16. H. Ehrig, A. Habel, H.-J. Kreowski, and F. Parisi-Presicce. Parallelism and concurrency in high level replacement systems. *MSCS*, 1:361–404, 1991.
17. H. Ehrig, A. Habel, J. Padberg, and U. Prange. Adhesive high-level replacement systems: A new categorical framework for graph transformation. *Fundamenta Informaticae*, 2006. To appear.
18. A. Habel and K.-H. Pennemann. Nested constraints and application conditions for high-level structures. In *Formal Methods in Software and System Modeling*, volume 3393 of *LNCS*, pages 293–308. Springer, 2005.
19. A. Habel and K.-H. Pennemann. Satisfiability of high-level conditions. In *Graph Transformations (ICGT'06)*, volume 4178 of *LNCS*, pages 430–444. Springer, 2006.
20. A. Habel, K.-H. Pennemann, and A. Rensink. Weakest preconditions for high-level programs. In *Graph Transformations (ICGT'06)*, volume 4178 of *LNCS*, pages 445–460. Springer, 2006.
21. A. Habel and D. Plump. Computational completeness of programming languages based on graph transformation. In *Proc. Foundations of Software Science and Computation Structures*, volume 2030 of *LNCS*, pages 230–245. Springer, 2001.
22. J. Y. Halpern and M. Y. Vardi. Model checking vs. theorem proving: A manifesto. In J. Allen, R. Fikes, and E. Sandewall, editors, *Proc. International Conference on Principles of Knowledge Representation and Reasoning*, pages 325–334. Morgan Kaufmann Publishers, 1991.
23. R. Heckel and A. Wagner. Ensuring consistency of conditional graph grammars. In *SEGRAGRA'95*, volume 2 of *ENTCS*, pages 95–104, 1995.
24. M. Koch, L. V. Mancini, and F. Parisi-Presicce. Graph-based specification of access control policies. *Journal of Computer and System Sciences (JCSS)*, 71:1–33, 2005.

25. B. König and V. Kozioura. Counterexample-guided abstraction refinement for the analysis of graph transformation systems. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 3920 of *LNCS*, pages 197–211. Springer, 2006.
26. S. Lack and P. Sobocinski. Adhesive categories. In *Foundations of Software Science and Computation Structures (FOSSACS'04)*, volume 2987 of *LNCS*, pages 273–288. Springer, 2004.
27. K. L. McMillan. Using unfoldings to avoid the state explosion problem in the verification of asynchronous circuits. In *Fourth Workshop on Computer-Aided Verification (CAV)*, volume 663 of *LNCS*, pages 164–174. Springer, 1992.
28. S. Owre, J. M. Rushby, and N. Shankar. PVS: A prototype verification system. In *11th International Conference on Automated Deduction (CADE)*, volume 607 of *LNCS*, pages 748–752. Springer, 1992.
29. D. Plump. Termination of graph rewriting is undecidable. *Fundamenta Informaticae*, 33(2):201–209, 1998.
30. D. Plump and S. Steinert. Towards graph programs for graph algorithms. In *Graph Transformations (ICGT'04)*, volume 3256 of *LNCS*, pages 128–143. Springer, 2004.
31. A. Rensink. Towards model checking graph grammars. In M. Leuschel, S. Gruner, and S. L. Presti, editors, *Workshop on Automated Verification of Critical Systems (AVoCS)*, Technical Report DSSE-TR-2003-2, pages 150–160. University of Southhampton, 2003.
32. A. Rensink. The GROOVE simulator: A tool for state space generation. In *Applications of Graph Transformations with Industrial Relevance (AGTIVE)*, volume 3062 of *LNCS*, page 485. Springer, 2004.
33. A. Rensink. Representing first-order logic by graphs. In *Graph Transformations (ICGT'04)*, volume 3256 of *LNCS*, pages 319–335. Springer, 2004.
34. A. Rensink, Á. Schmidt, and D. Varró. Model checking graph transformations: A comparison of two approaches. In *Graph Transformations (ICGT'04)*, volume 3256 of *LNCS*, pages 226–241. Springer, 2004.
35. D. Varró. Towards symbolic analysis of visual modeling languages. *ENTCS*, 72(3), 2003.
36. D. Varró. Automated formal verification of visual modeling languages by model checking. *Journal of Software and Systems Modelling*, 3(2):85–113, 2004.

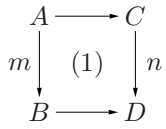
A Weak Adhesive HLR Categories

We recall the notions of weak adhesive high-level replacement (HLR) categories. Adhesive HLR-sytstems, a combination of HLR-systems and adhesive categories, are systematically studied in [17,15].

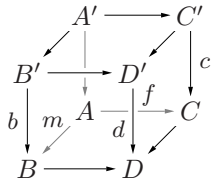
Definition 6 (weak adhesive HLR category). A category $\mathcal{C}$ with a morphism class $\mathcal{M}$ is called *weak adhesive HLR category*, if the following properties hold.

(1) $\mathcal{M}$ is a class of monomorphisms closed under compositions and decompositions, i.e. $f \in \mathcal{M}$, $g \in \mathcal{M}$ implies $g \circ f \in \mathcal{M}$ and $g \circ f \in \mathcal{M}$, $g \in \mathcal{M}$ implies $f \in \mathcal{M}$.

(2) $\mathcal{C}$ has pushouts and pullbacks along $\mathcal{M}$-morphisms, i.e. pushouts and pullbacks, where at least one of the given morphisms is in $\mathcal{M}$, and $\mathcal{M}$-morphisms are closed under pushouts and pullbacks, i.e. given a pushout (1), $m \in \mathcal{M}$ implies $n \in \mathcal{M}$ and, given a pullback (1), $n \in \mathcal{M}$ implies $m \in \mathcal{M}$.



(3) Pushouts in $\mathcal{C}$ along $\mathcal{M}$-morphisms are weak VK-squares, i.e. for any commutative cube in $\mathcal{C}$ where we have the pushout with $m \in \mathcal{M}$ and ($f \in \mathcal{M}$ or $b, c, d \in \mathcal{M}$) in the bottom and the back faces are pullbacks, it holds: the top is pushout iff the front faces are pullbacks.

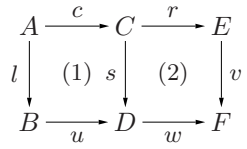


Example 10. Examples of weak adhesive categories are the category $\langle \mathbf{Graph}, \mathcal{M} \rangle$ of graphs with class $\mathcal{M}$ of all injective graph morphisms and the category $\langle \mathbf{Spec}, \mathcal{M} \rangle$ of algebraic specifications with class $\mathcal{M}$ of all strict injective specification morphisms.

Weak adhesive HLR-categories have a number of nice properties, called HLR properties [16].

Fact 3 (HLR properties of adhesive HLR categories). Given a weak adhesive HLR-category $\langle \mathcal{C}, \mathcal{M} \rangle$, the following HLR conditions are satisfied.

(1) Pushouts along $\mathcal{M}$-morphisms are pullbacks.
(2) Pushout-pullback decomposition. If the diagram (1)+(2) is a pushout, (2) a pullback, $w \in \mathcal{M}$ and ($l \in \mathcal{M}$ or $c \in \mathcal{M}$), then (1) and (2) are pushouts and also pullbacks.



(3) Uniqueness of pushout complements for $\mathcal{M}$-morphisms. Given morphisms $c\colon A \to C$ in $\mathcal{M}$ and $s\colon C \to D$, then there is up to isomorphism at most one B with $l\colon A \to B$ and $u\colon B \to D$ such that diagram (1) is a pushout.

Proof. See [26,17,15].

B Partial Derivations

In this section, we define the set of all partial derivations within the execution of a program P.

The semantic of programs does not suffice to give a formal notion of program termination. Therefore, we define the set of all partial derivations of a program starting form an object G. Beforehand, let D, D' be sets of derivations and define $D \cdot D' = \{d \Rightarrow^0 d' \mid d \in D, d' \in D' \text{ and } \mathrm{In}(d') \cong \mathrm{Res}(d)\}$, where $\mathrm{In}(G \Rightarrow^* H) = G$ and $\mathrm{Res}(G \Rightarrow^* H) = H$ for every derivation sequence $G \Rightarrow^* H$.

Definition 7 (partial derivations). Let $\mathrm{Der}(P)$ be the set of all *derivations* of a given program P, i.e. $G \Rightarrow^* H \in \mathrm{Der}(P)$ if and only if $\langle G, H\rangle \in [\![P]\!]$. The set of all *partial derivations* $\mathrm{PDer}(P)$ within the execution of a program P is defined inductively. For a rule p, for a finite set $\mathcal{S}$ of programs and programs P, Q, let

$$\begin{aligned}
\mathrm{PDer}(\texttt{Skip}) &= \mathrm{Der}(\texttt{Skip})\\
\mathrm{PDer}(p) &= \mathrm{PDer}(\texttt{Skip}) \cup \mathrm{Der}(p)\\
\mathrm{PDer}(\mathcal{S}) &= \textstyle\bigcup_{P\in\mathcal{S}} \mathrm{PDer}(P)\\
\mathrm{PDer}((P;Q)) &= \mathrm{PDer}(P) \cup \mathrm{Der}(P) \cdot \mathrm{PDer}(Q)\\
\mathrm{PDer}(P^*) &= \mathrm{Der}(P^*) \cdot \mathrm{PDer}(P)\\
\mathrm{PDer}(P\downarrow) &= \mathrm{PDer}(P^*)
\end{aligned}$$

Consider $\mathrm{Der}(P, G)$, $\mathrm{PDer}(P, G)$ to be restrictions of $\mathrm{Der}(P)$ and $\mathrm{PDer}(P)$ to derivations with input G.

Remark 5. PDer may consist of derivations which are not a part of any derivation in Der.

Example 11. Assume, $G \Rightarrow H$ in $\mathrm{Der}(P)$ and $\nexists M \in \mathcal{C}.\ H \Rightarrow M \in \mathrm{Der}(Q)$. Then the dead end $G \Rightarrow H$ is in $\mathrm{PDer}(P; Q)$, while it is not a part of any deriation in $\mathrm{Der}(P; Q)$.

The following lemma over sets of derivations is used in the proof of $\mathrm{Wtp}(P, \mathrm{true}) \equiv \mathrm{wtp}(P, \mathrm{true})$ in Appendix D.

Lemma 1 (set of derivations). *Let D_i be a set of derivations for every $i \in \mathbb{N}$. If $D_i = \emptyset$ implies $D_{i+1} = \emptyset$ and if $D_{i+1} \not\subseteq \bigcup_{j=0}^{i} D_j$ for every $i \in \mathbb{N}$, we have: $\bigcup_{i=0}^{\infty} D_i$ is finite implies there is a natural number $k \in \mathbb{N}$ such that $\bigcup_{i=0}^{\infty} D_i = \bigcup_{i=0}^{k} D_i$ and $D_{k+1} = \emptyset$.*

Proof. For every set of derivations D with $D_i = \emptyset$ implies $D_{i+1} = \emptyset$, we have $D_{i+1} \neq \emptyset$ implies $D_i \neq \emptyset$. Assume, there does not exists a $k \in \mathbb{N}$ such that $D_{k+1} = \emptyset$. Then $D_{k+1} \neq \emptyset$ for every k and, as $d \in D_{k+1}$ implies $d \notin \bigcup_{i=0}^{k} D_i$ at least for some d, we have $|\bigcup_{i=0}^{k} D_i| \geq k$ and finally $\bigcup_{i=0}^{\infty} D_i$ is infinite, contradiction.

C Properties of Weakest Preconditions

In this section, we give some essential properties of weakest preconditions and present general facts on implication and equivalence of conditions.

Fact 4 (properties of weakest preconditions).

(1) wlp *is universally conjunctive*: $\mathrm{wlp}(P, d \wedge d') \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wlp}(P, d')$
(2) wlp *is a subcondition of* wp: $\mathrm{wp}(P, d \wedge d') \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wp}(P, d')$
(3) wlp *is a subcondition of* wtp: $\mathrm{wtp}(P, d \wedge d') \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wtp}(P, d')$
(4) wlp *and* wtp *are subconditions of* $\mathrm{wp}(P, \mathrm{true})$:
$$\mathrm{wp}(P, d) \equiv \neg\mathrm{wlp}(P, \mathrm{false}) \wedge \mathrm{wtp}(P, d)$$
(5) wlp *is monotonic*: $d \Rightarrow d'$ implies $\mathrm{wlp}(P, d) \Rightarrow \mathrm{wlp}(P, d')$

Proof. Property (1) "wlp is universally conjunctive":

$G \models \mathrm{wlp}(P, d \wedge d')$
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models (d \wedge d'))$ (Def. wlp)
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow (H \models d \wedge H \models d'))$ (Def. $\models$)
$\Leftrightarrow \forall H.\ ((\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d) \wedge (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d'))$ $(\substack{(F \Rightarrow (G \wedge H)) \equiv \\ (F \Rightarrow G) \wedge (F \Rightarrow H)})$
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d) \wedge \forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d')$ $(\substack{\forall x F \wedge G \equiv \\ \forall x F \wedge \forall x G})$
$\Leftrightarrow G \models \mathrm{wlp}(P, d) \wedge G \models \mathrm{wlp}(P, d')$ (Def. wlp)
$\Leftrightarrow G \models \mathrm{wlp}(P, d) \wedge \mathrm{wlp}(P, d').$ (Def. $\models$)

Property (2) "wlp is a subcondition of wp": First, $\mathrm{wp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wp}(P, \mathrm{true})$ because for every object $G \in \mathcal{C}$, G satisfies $\mathrm{wp}(P, \mathrm{true})$, if and only if properties (1)-(3) are satisfied for d (see Definition 5), if and only if properties (1) is satisfied for d and properties (1)-(3) are satisfied for true, if and only if G satisfies $\mathrm{wlp}(P, d)$ and $\mathrm{wp}(P, \mathrm{true})$ (Definition 5). Furthermore:

$\mathrm{wp}(P, d \wedge d')$
$\equiv \mathrm{wlp}(P, d \wedge d') \wedge \mathrm{wp}(P, \mathrm{true})$ ($\mathrm{wp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wp}(P, \mathrm{true})$)
$\equiv \mathrm{wlp}(P, d) \wedge \mathrm{wlp}(P, d') \wedge \mathrm{wp}(P, \mathrm{true})$ (Fact 4.(1))
$\equiv \mathrm{wlp}(P, d) \wedge \mathrm{wp}(P, d')$ ($\mathrm{wp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wp}(P, \mathrm{true})$)

Property (3) "wlp is a subcondition of wtp": First, $\mathrm{wtp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wtp}(P, \mathrm{true})$ because for every object $G \in \mathcal{C}$, G satisfies $\mathrm{wtp}(P, d)$, if and only if properties (1) and (3) are satisfied for d (see Definition 5), if and only if property (1) is satisfied for d and (1) and (3) are satisfied for true, if and only if G satisfies $\mathrm{wlp}(P, d)$ and $\mathrm{wtp}(P, \mathrm{true})$ (Definition 5). Furthermore:

$\mathrm{wtp}(P, d \wedge d')$
$\equiv \mathrm{wlp}(P, d \wedge d') \wedge \mathrm{wtp}(P, \mathrm{true})$ ($\mathrm{wtp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wtp}(P, \mathrm{true})$)
$\equiv \mathrm{wlp}(P, d) \wedge \mathrm{wlp}(P, d') \wedge \mathrm{wtp}(P, \mathrm{true})$ (Fact 4.(1))
$\equiv \mathrm{wlp}(P, d) \wedge \mathrm{wtp}(P, d')$ ($\mathrm{wtp}(P, d) \equiv \mathrm{wlp}(P, d) \wedge \mathrm{wtp}(P, \mathrm{true})$)

Property (4) "wlp and wtp are subconditions of wp": For every object $G \in \mathcal{C}$, G satisfies $\mathrm{wp}(P, d)$, if and only if properties (1)-(3) are satisfied for d (see Definition 5), if and only if property (2) is satisfied, and (1), (3) are satisfied for d, if and only if G satisfies $\neg\mathrm{wlp}(P, \mathrm{false})$ and $\mathrm{wtp}(P, d)$ (Fact 2 and Definition 5).

Finally, property (5) "wlp is monotonic": $G \models \mathrm{wlp}(P, d)$ if and only if $\forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d)$, by assumption implies $\forall H.\ (\langle G, H\rangle \in [\![p]\!] \Rightarrow H \models d')$ if and only if $G \models \mathrm{wlp}(P, d')$.

For the Example 9 in Section 4, we use the following facts on conditions.

Fact 5 (equivalences and implications).

(1) Let I be the $\mathcal{M}$-inital object, $i\colon I \to C$ be the unique $\mathcal{M}$-morphism with codomain C, and let c_x be a condition over C for every index $x \in X$. Then we have,

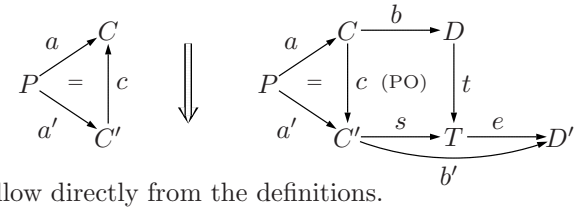
$$\begin{array}{lcl} \exists(i, \vee_{x\in X}\, c_x) & \equiv & \vee_{x\in X}\, \exists(i, c_x) \\ \forall(i, \wedge_{x\in X}\, c_x) & \equiv & \wedge_{x\in X}\, \forall(i, c_x) \\ \exists(i, \wedge_{x\in X}\, c_x) & \text{implies} & \wedge_{x\in X}\, \exists(i, c_x) \\ \forall(i, \vee_{x\in X}\, c_x) & \text{if} & \vee_{x\in X}\, \forall(i, c_x). \end{array}$$

(2) For every morphism $b \circ a$ and condition c over the codomain of b,

$$\begin{array}{l} \exists(a, \exists(b, c)) \equiv \exists(b \circ a, c) \\ \forall(a, \forall(b, c)) \equiv \forall(b \circ a, c). \end{array}$$

(3) A condition $\exists(P \xrightarrow{a} C)$ implies $\exists(P \xrightarrow{a'} C')$ on objects as well as morphisms with domain P, if there is a $\mathcal{M}$-morphism $C' \xrightarrow{c} C$ such that $a = c \circ a'$.

(4) A condition $\forall(P \xrightarrow{a} C,\ \bigvee_{b\in B} \exists(C \xrightarrow{b} D))$ implies $\forall(P \xrightarrow{a'} C',\ \bigvee_{b'\in B'} \exists(C \xrightarrow{b'} D'))$ on objects as well as morphisms with domain P, if there is a $\mathcal{M}$-morphism $C \xrightarrow{c} C'$ such that $a' = c \circ a$ and if for every $b \in B$ with $s \circ c = t \circ b$ being the associated pushout, and every epimorphism $T \xrightarrow{e} D'$ with both $e \circ s$ and $e \circ t$ in $\mathcal{M}$, there is a morphism $b' \in B'$ with $b' = e \circ s$.



Proof. (1) and (2) follow directly from the definitions.

(3) For a morphism $P \xrightarrow{p} G$ we observe: p satisfies $\exists(P \xrightarrow{a} C)$, implies there exist a $\mathcal{M}$-morphism $C \xrightarrow{q} G$ with $p = q \circ a$, implies there exist a $\mathcal{M}$-morphism $C' \xrightarrow{q'} G$ with $p = q' \circ a'$ where $q' = q \circ c$ (q' in $\mathcal{M}$ as $\mathcal{M}$ closed under composition), implies p satisfies $\exists(P \xrightarrow{a'} C')$.

(4) For a morphism $P \xrightarrow{p} G$ we observe: p satisfies $\forall(P \xrightarrow{a} C,\ \bigvee_{b\in B} \exists(C \xrightarrow{b} D))$, implies for all $\mathcal{M}$-morphisms $C \xrightarrow{q} G$ with $p = q \circ a$ there exists a $\mathcal{M}$-morphism $D \xrightarrow{r} G$ for some $b \in B$ with $q = r \circ b$. For every $\mathcal{M}$-morphism $C' \xrightarrow{q'} G$ with $p = q' \circ a'$, define the $\mathcal{M}$-morphism $C \xrightarrow{q} G$ by $q = q' \circ c$ (q in $\mathcal{M}$ as $\mathcal{M}$ closed under composition). We observe $p = q' \circ a' = q' \circ c \circ a = q \circ a$. By assumption there exists a $\mathcal{M}$-morphism $D \xrightarrow{r} G$ with $q = r \circ b$ for some $b \in B$. Construct the pushout $s \circ c = t \circ b$. By definition of pushouts,

there exists a (unique) morphism $T \xrightarrow{h} G$ with $q' = h \circ s$. Consider the epi-$\mathcal{M}$-factorization $r' \circ e = h$ with epimorphism e and $\mathcal{M}$-morphism r'. By assumption there is a morphism $b' = e \circ s$ in B'. Therefore, p satisfies $\forall(P \xrightarrow{a} C,\ \bigvee_{b' \in B'} \exists(C \xrightarrow{b'} D))$.

For the exemplary proof in Section 4, the following lemma is essential:

Lemma 2 (invariants). *For every program p and condition d we have:*
If d implies $\mathrm{Wlp}(P, d)$ *then d* implies $\mathrm{Wlp}(P^*, d)$ *as well as d* implies $\mathrm{Wlp}(P{\downarrow}, d)$.

Proof. By definition $\mathrm{Wlp}(P^*, d) = \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, d)$. Using the fact d implies $\mathrm{Wlp}(P, d)$, one can show by induction over i, d implies $\mathrm{Wlp}(P^i, d)$ for every $i \in \mathbb{N}$. By definition $\mathrm{Wlp}(P{\downarrow}, d) = \mathrm{Wlp}(P^*, \mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d)$ and with d implies $(\mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d)$ we conclude $\mathrm{Wlp}(P^*, d)$ implies $\mathrm{Wlp}(P^*, \mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d)$ (see Fact 4.(5)).

D Proof

In this Section, we present the missing parts of the proofs of Theorems 5 and 6.

Proof of Theorems 5 and 6. We continue to show $\mathrm{Wlp}(P, d) \equiv \mathrm{wlp}(P, d)$ and $\mathrm{Wtp}(P, d) \equiv \mathrm{wtp}(P, d)$. The proofs are done by induction over the structure of programs, the basis was given in Section 4. Induction hypothesis: assume the statements hold for a set of programs $\mathcal{S}$ and for programs P, Q. For the induction step, we have to distinguish the following cases:

For `Skip`, we have

$$
\begin{aligned}
& G \models \mathrm{wlp}(\texttt{Skip}, d) \\
\Leftrightarrow\ & \forall H.\ (\langle G, H\rangle \in [\![\texttt{Skip}]\!] \Rightarrow H \models d) && \text{(Def. wlp)} \\
\Leftrightarrow\ & \forall H.\ (G \cong H \Rightarrow H \models d) && \text{(Def. } [\![\texttt{Skip}]\!]\text{)} \\
\Leftrightarrow\ & G \models d. && (G \cong H)
\end{aligned}
$$

Every application of `Skip` terminates, hence wtp reduces to wlp. For the nondeterministic choice $\mathcal{S}$, we have

$$
\begin{aligned}
& G \models \mathrm{wlp}(\mathcal{S}, d) \\
\Leftrightarrow\ & \forall H.\ (\langle G, H\rangle \in [\![\mathcal{S}]\!] \Rightarrow H \models d) && \text{(Def. wlp)} \\
\Leftrightarrow\ & \forall H.\ (\langle G, H\rangle \in \textstyle\bigcup_{P \in \mathcal{S}} [\![P]\!] \Rightarrow H \models d) && \text{(Def. } [\![\mathcal{S}]\!]\text{)} \\
\Leftrightarrow\ & \forall H.\ (\textstyle\bigvee_{P \in \mathcal{S}} \langle G, H\rangle \in [\![P]\!] \Rightarrow H \models d) && \text{(Def. } \cup\text{)} \\
\Leftrightarrow\ & \forall H.\ \textstyle\bigwedge_{P \in \mathcal{S}} (\langle G, H\rangle \in [\![P]\!] \Rightarrow H \models d) && \left(\begin{smallmatrix}(F \vee G) \Rightarrow H \equiv \\ (F \Rightarrow H) \wedge (G \Rightarrow H)\end{smallmatrix}\right) \\
\Leftrightarrow\ & \textstyle\bigwedge_{P \in \mathcal{S}} \forall H.\ (\langle G, H\rangle \in [\![P]\!] \Rightarrow H \models d) && \left(\begin{smallmatrix}\forall x F \wedge G \equiv \\ \forall x F \wedge \forall x G\end{smallmatrix}\right) \\
\Leftrightarrow\ & \textstyle\bigwedge_{P \in \mathcal{S}} G \models \mathrm{Wlp}(P, d) && \text{(Def. wlp, IH. } P\text{)} \\
\Leftrightarrow\ & G \models \textstyle\bigwedge_{P \in \mathcal{S}} \mathrm{Wlp}(P, d). && \text{(Def. } \models\text{)}
\end{aligned}
$$

$$
\begin{aligned}
& G \models \mathrm{wtp}(\mathcal{S}, \mathrm{true}) \\
\Leftrightarrow\ & \mathrm{PDer}(\mathcal{S}) \text{ is finite} && \text{(Def. wtp)} \\
\Leftrightarrow\ & (\textstyle\bigcup_{P \in \mathcal{S}} \mathrm{PDer}(P, G)) \text{ is finite} && \text{(Def. PDer)} \\
\Leftrightarrow\ & \textstyle\bigwedge_{P \in \mathcal{S}} (\mathrm{PDer}(P, G) \text{ is finite}) && \text{(Def. is finite)}
\end{aligned}
$$

$\Leftrightarrow \bigwedge_{P\in\mathcal{S}}\ G \models \mathrm{Wtp}(P,\mathrm{true})$ (Def.wtp, IH. P)
$\Leftrightarrow G \models \bigwedge_{P\in\mathcal{S}}\ \mathrm{Wtp}(P,\mathrm{true})$. (Def.$\models$)

$\mathrm{Wtp}(\mathcal{S},d) \equiv \mathrm{wtp}(\mathcal{S},d)$, because $\mathrm{Wtp}(\mathcal{S},d)$ is defined as $\bigwedge_{P\in\mathcal{S}} \mathrm{Wtp}(P,d)$, which is, by induction hypothesis equivalent to $\bigwedge_{P\in\mathcal{S}} \mathrm{wtp}(P,d)$, which is, by Fact 4.(3), equivalent to $\bigwedge_{P\in\mathcal{S}}(\mathrm{wlp}(P,d) \wedge \mathrm{wtp}(P,\mathrm{true}))$, equivalent to $\bigwedge_{P\in\mathcal{S}} \mathrm{wlp}(P,d) \wedge \bigwedge_{P\in\mathcal{S}} \mathrm{wtp}(P,\mathrm{true})$, which is, by induction hypothesis, equivalent to $\mathrm{wlp}(\mathcal{S},d) \wedge \mathrm{wtp}(\mathcal{S},\mathrm{true})$, which is, by Fact 4.(3), equivalent to $\mathrm{wtp}(\mathcal{S},d)$. For the sequential composition $(P;Q)$, we have

$G \models \mathrm{wlp}((P;Q),d)$
$\Leftrightarrow \forall H.\ (\langle G,H\rangle \in [\![(P;Q)]\!] \Rightarrow H \models d)$ (Def. wlp)
$\Leftrightarrow \forall H.\ (\langle G,H\rangle \in [\![Q]\!] \circ [\![P]\!] \Rightarrow H \models d)$ (Def. $[\![(P;Q)]\!]$)
$\Leftrightarrow \forall H.\ \forall M.\ ((\langle G,M\rangle \in [\![P]\!] \wedge \langle M,H\rangle \in [\![Q]\!]) \Rightarrow H \models d)$ (Def. $\circ$)
$\Leftrightarrow \forall M.\ \forall H.\ (\langle G,M\rangle \in [\![P]\!] \Rightarrow (\langle M,H\rangle \in [\![Q]\!] \Rightarrow H \models d))$ $(\overset{(F\wedge G)\Rightarrow H\equiv}{(F\Rightarrow(G\Rightarrow H))})$
$\Leftrightarrow \forall M.\ (\langle G,M\rangle \in [\![P]\!] \Rightarrow \forall H.\ (\langle M,H\rangle \in [\![Q]\!] \Rightarrow H \models d))$ $(\overset{x\notin\mathrm{Free}(F):\forall x(F\vee G)}{\equiv F\vee\forall x G})$
$\Leftrightarrow \forall M.\ (\langle G,M\rangle \in [\![P]\!] \Rightarrow M \models \mathrm{Wlp}(Q,d))$ (Def. wlp, IH. Q)
$\Leftrightarrow G \models \mathrm{Wlp}(P,\mathrm{Wlp}(Q,d))$. (Def. wlp, IH. P)

$G \models \mathrm{wtp}((P;Q),\mathrm{true})$
$\Leftrightarrow \mathrm{PDer}((P;Q),G)$ is finite (Def. wtp)
$\Leftrightarrow \mathrm{PDer}(P,G) \cup \mathrm{Der}(P,G)\cdot\mathrm{PDer}(Q)$ is finite (Def. PDer)
$\Leftrightarrow \mathrm{PDer}(P,G)$ is finite $\wedge\ \mathrm{Der}(P,G)\cdot\mathrm{PDer}(Q)$ is finite (Def. is finite)
$\Leftrightarrow$ $\mathrm{PDer}(P,G)$ is finite (Def. $\mathrm{Der}(P,G)$)
$\quad\wedge\ \forall H.\ G \Rightarrow^* H \in \mathrm{Der}(P,G) \Rightarrow \mathrm{PDer}(Q,H)$ is finite
$\Leftrightarrow G \models \mathrm{Wtp}(P,\mathrm{true}) \wedge G \models \mathrm{Wlp}(P,\mathrm{Wtp}(Q,\mathrm{true}))$ $(\overset{\text{Def.wtp, IH. } P,Q,}{\text{Def. wlp, IH. } P})$
$\Leftrightarrow G \models \mathrm{Wtp}(P,\mathrm{true}) \wedge \mathrm{Wlp}(P,\mathrm{Wtp}(Q,\mathrm{true}))$ (Def.$\models$)
$\Leftrightarrow G \models \mathrm{Wtp}(P,\mathrm{Wtp}(Q,\mathrm{true}))$. (Def.wtp)

We have $\mathrm{Wtp}((P;Q),d) \equiv \mathrm{wtp}((P;Q),d)$, because $\mathrm{Wtp}((P;Q),d)$ is defined as $\mathrm{Wtp}(P,\mathrm{Wtp}(Q,d))$, by induction hypothesis, equivalent to $\mathrm{wtp}(P,\mathrm{wtp}(Q,d))$, which is, by Fact 4.(3), equivalent to $\mathrm{wtp}(P,\mathrm{wlp}(Q,d)\wedge\mathrm{wtp}(Q,\mathrm{true}))$, which is, by Fact 4.(3), equivalent to $\mathrm{wlp}(P,\mathrm{wlp}(Q,d)) \wedge \mathrm{wtp}(P,\mathrm{wtp}(Q,\mathrm{true}))$, which is, by induction hypothesis, equivalent to $\mathrm{wlp}((P;Q),d) \wedge \mathrm{wtp}((P;Q),\mathrm{true})$, which is, by Fact 4.(3), equivalent to $\mathrm{wtp}((P;Q),d)$. For the reflexive, transitive closure of a program P, the weakest liberal precondition $\mathrm{wlp}(P^*,d)$ may be described as a non finite representation:

$G \models \mathrm{wlp}(P^*,d)$
$\Leftrightarrow \forall H.\ (\langle G,H\rangle \in [\![P^*]\!] \Rightarrow H \models d)$ (Def. wlp)
$\Leftrightarrow \forall H.\ (\langle G,H\rangle \in [\![P]\!]^* \Rightarrow H \models d)$ (Def. $[\![P^*]\!]$)
$\Leftrightarrow \forall H.\ (\langle G,H\rangle \in \bigcup_{i=0}^{\infty} [\![P^i]\!] \Rightarrow H \models d)$ (Def. $*$)
$\Leftrightarrow \forall H.\ (\bigvee_{i=0}^{\infty}(\langle G,H\rangle \in [\![P^i]\!]) \Rightarrow H \models d)$ (Def. $\bigcup$)
$\Leftrightarrow \forall H.\ (\bigwedge_{i=0}^{\infty}(\langle G,H\rangle \in [\![P^i]\!] \Rightarrow H \models d))$ $(\overset{((F\vee G)\Rightarrow H)}{(F\Rightarrow H)\wedge(G\Rightarrow H)})$
$\Leftrightarrow \bigwedge_{i=0}^{\infty} \forall H.\ (\langle G,H\rangle \in [\![P^i]\!] \Rightarrow H \models d)$ $(\overset{\forall xF\wedge\forall xG}{\equiv\forall xF\wedge G})$
$\Leftrightarrow \bigwedge_{i=0}^{\infty} G \models \mathrm{Wlp}(P^i,d)$ (Def. wlp, IH. P)
$\Leftrightarrow G \models \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i,d)$. (Def. $\models$)

where for $i \geq 0$, P^i is inductively defined by `Skip` for $i = 0$ and by $P^{i+1} = P^i; P$.

$G \models \mathrm{wtp}(P^*, \mathrm{true})$
$\Leftrightarrow \mathrm{PDer}(P^*, G)$ is finite (Def. wtp)
$\Leftrightarrow \mathrm{Der}(P^*, G) \cdot \mathrm{PDer}(P)$ is finite (Def. $\mathrm{PDer}(P^*)$)
$\Leftrightarrow (\bigcup_{i=0}^{\infty} \mathrm{Der}(P^i, G)) \cdot \mathrm{PDer}(P)$ is finite (Def. $\mathrm{Der}(P^*)$, Def. $*$)
$\Leftrightarrow (\bigcup_{i=0}^{\infty} \mathrm{Der}(P^i, G) \cdot \mathrm{PDer}(P))$ is finite (Def. $D \cdot D'$)
$\Leftrightarrow \bigvee_{k=0}^{\infty}((\bigcup_{i=0}^{k} \mathrm{Der}(P^i, G) \cdot \mathrm{PDer}(P)) \text{ is finite}$ (Lem. 1, $\Rightarrow \mathrm{Der}(P^{i+1},G)\cdot\mathrm{PDer}(P)=\emptyset$)
$\quad \wedge \mathrm{Der}(P^{k+1}, G) \cdot \mathrm{PDer}(P) = \emptyset)$
$\Leftrightarrow \bigvee_{k=0}^{\infty} \begin{pmatrix} \bigwedge_{i=0}^{k} (\mathrm{Der}(P^i, G) \cdot \mathrm{PDer}(P) \text{ is finite}) \\ \wedge \mathrm{Der}(P^{k+1}, G) = \emptyset \end{pmatrix}$ ($\Rightarrow \mathrm{Der}(P^i,G)=\emptyset$)
$\Leftrightarrow \bigvee_{k=0}^{\infty} \begin{pmatrix} \bigwedge_{i=0}^{k} G \models \mathrm{Wlp}(P^i, \mathrm{Wtp}(P, \mathrm{true})) \\ \wedge\ G \models \mathrm{Wlp}(P^k, \mathrm{Wlp}(P, \mathrm{false})) \end{pmatrix}$ (Def. wtp, IH. P, Def. wlp, IH. P)
$\Leftrightarrow G \models \bigvee_{k=0}^{\infty}(\bigwedge_{i=0}^{k} \mathrm{Wlp}(P^i, \mathrm{Wtp}(P, \mathrm{true})) \wedge \mathrm{Wlp}(P^k, \mathrm{Wlp}(P, \mathrm{false})))$ (Def. $\models$)
$\Leftrightarrow G \models \bigvee_{k=0}^{\infty}(\bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, \mathrm{Wtp}(P, \mathrm{true})) \wedge \mathrm{Wlp}(P^k, \mathrm{Wlp}(P, \mathrm{false})))$ $(*)$
$\Leftrightarrow G \models \bigvee_{k=0}^{\infty} \mathrm{Wlp}(P^k, \mathrm{Wlp}(P, \mathrm{false}))\ \wedge\ \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, \mathrm{Wtp}(P, \mathrm{true}))$. ($i$ indepen.)

where Lemma 1 is given below and $(*)$ is:

$$\mathrm{wlp}(P^{k+1}, \mathrm{false}) \text{ implies } \bigwedge_{i=k+1}^{\infty} \mathrm{wlp}(P^i, \mathrm{wtp}(P, \mathrm{true})).$$

This can be seen as follows $G \models \mathrm{wlp}(P^{k+1}, \mathrm{false})$ implies $\mathrm{Der}(P^{k+1}, G) = \emptyset$, implies $\mathrm{Der}(P^{k+1}, G) \cdot \mathrm{PDer}(P) = \emptyset$, implies $\mathrm{Der}(P^i, G) \cdot \mathrm{PDer}(P) = \emptyset$ for $i \geq k+1$, implies $\mathrm{wlp}(P^i, \mathrm{wtp}(P, \mathrm{true}))$ for $i \geq k+1$.

$\mathrm{Wtp}(P^*, d) \equiv \mathrm{wtp}(P^*, d)$, as $\mathrm{Wtp}(P^*, d)$ is defined by $\bigvee_{k=0}^{\infty} \mathrm{Wlp}(P^{k+1}, \mathrm{false}) \wedge \bigwedge_{i=0}^{\infty} \mathrm{Wlp}(P^i, d \wedge \mathrm{Wtp}(P, \mathrm{true}))$, which is, by induction hypothesis equivalent to $\bigvee_{k=0}^{\infty} \mathrm{wlp}(P^{k+1}, \mathrm{false}) \wedge \bigwedge_{i=0}^{\infty} \mathrm{wlp}(P^i, d \wedge \mathrm{wtp}(P, \mathrm{true}))$, which is, by Fact 4.(3), equivalent to $\bigvee_{k=0}^{\infty} \mathrm{wlp}(P^{k+1}, \mathrm{false}) \wedge \bigwedge_{i=0}^{\infty} \mathrm{wlp}(P^i, d) \wedge \bigwedge_{i=0}^{\infty} \mathrm{wlp}(P^i, \mathrm{wtp}(P, \mathrm{true}))$, which is, by correctness of Wlp and $\mathrm{Wtp}(P^*, \mathrm{true})$, equivalent to $\mathrm{wlp}(P^*, d) \wedge \mathrm{wtp}(P^*, \mathrm{true})$, which is, by Fact 4.(3), equivalent to $\mathrm{wtp}(P^*, d)$.

The problem to find a weakest precondition for an iteration of P (as long as possible) may be reduced to the problem for the reflexive, transitive closure P^*:

$G \models \mathrm{wlp}(P\downarrow, d)$
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![P\downarrow]\!] \Rightarrow H \models d)$ (Def. wlp)
$\Leftrightarrow \forall H.\ ((\langle G, H\rangle \in [\![P]\!]^* \wedge \nexists M.\ (\langle H, M\rangle \in [\![P]\!])) \Rightarrow H \models d)$ (Def. $[\![P\downarrow]\!]$)
$\Leftrightarrow \forall H.\ ((\langle G, H\rangle \in [\![P]\!]^* \wedge \forall M.\ (\langle H, M\rangle \in [\![P]\!]) \Rightarrow \mathrm{false}) \Rightarrow H \models d)$ ($\equiv \forall x \neg F$)
$\Leftrightarrow \forall H.\ ((\langle G, H\rangle \in [\![P]\!]^* \wedge H \models \mathrm{Wlp}(P, \mathrm{false})) \Rightarrow H \models d)$ (Def. wp, IH. P)
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![P]\!]^* \Rightarrow (H \models \mathrm{Wlp}(P, \mathrm{false}) \Rightarrow H \models d))$ ($F \Rightarrow (G \Rightarrow H)$)
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![P]\!]^* \Rightarrow H \models (\mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d))$ (Def. $\models$)
$\Leftrightarrow \forall H.\ (\langle G, H\rangle \in [\![P^*]\!] \Rightarrow H \models (\mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d))$ (Def. $[\![P^*]\!]$)
$\Leftrightarrow G \models \mathrm{Wlp}(P^*, \mathrm{Wlp}(P, \mathrm{false})) \Rightarrow d)$. (Def. wlp, IH. P^*)

We have $\mathrm{Wtp}(P\downarrow, \mathrm{true}) \equiv \mathrm{wtp}(P\downarrow, \mathrm{true})$, because $\mathrm{Wtp}(P\downarrow, \mathrm{true})$ is defined as $\mathrm{Wtp}(P^*, \neg\mathrm{Wlp}(P, \mathrm{false}) \Rightarrow \mathrm{true})$, which is, by induction hypothesis, equivalent to $\mathrm{wtp}(P^*, \neg\mathrm{wlp}(P, \mathrm{false}) \Rightarrow \mathrm{true})$, which is equivalent to $\mathrm{wtp}(P^*, \mathrm{true})$, which is, by Definitions 4 and 7, equivalent to $\mathrm{wtp}(P\downarrow, \mathrm{true})$.

$\mathrm{Wtp}(P\downarrow, d)$
$\equiv \mathrm{Wtp}(P^*, \mathrm{Wlp}(P, \mathrm{false}) \Rightarrow d)$ (Def. Wtp)
$\equiv \mathrm{wtp}(P^*, \mathrm{wlp}(P, \mathrm{false}) \Rightarrow d)$ (IH. P^*, P)

$\equiv \mathrm{wlp}(P^*, \mathrm{wlp}(P, \mathrm{false}) \Rightarrow d) \wedge \mathrm{wtp}(P^*, \mathrm{true})$ (Fact 4.(3))
$\equiv \mathrm{wlp}(P^*, \mathrm{wlp}(P, \mathrm{false}) \Rightarrow d) \wedge \mathrm{wtp}(P^*, \mathrm{wlp}(P, \mathrm{false}) \Rightarrow \mathrm{true})$ $((F \Rightarrow \mathrm{true}) \equiv \mathrm{true})$
$\equiv \mathrm{wlp}(P{\downarrow}, d) \wedge \mathrm{wtp}(P{\downarrow}, \mathrm{true})$ (Def. wlp, wtp, IH. $P{\downarrow}$)
$\equiv \mathrm{wtp}(P{\downarrow}, d)$ (Fact 4.(3))

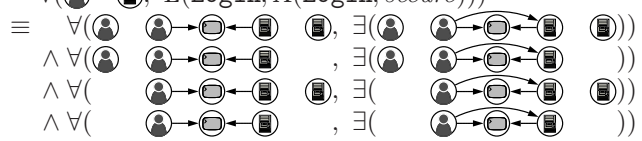
E Access Control System

In this Section, we continue Example 9. We are investigating, whether or not *secure* is invariant. For a proof, we have to show *secure* implies Wlp(P, *secure*) for every program $P \in$ `Control`. So far, we have found proofs for the programs `AddUser` and `Grant`.

We also have *secure* implies Wlp(`Login`, *secure*). The proof is similar to the one for `Grant`, as L(`Grant`, A(`Grant`, *secure*)) is similar to L(`Login`, A(`Login`, *secure*)):

L(`Login`, A(`Login`, *secure*))

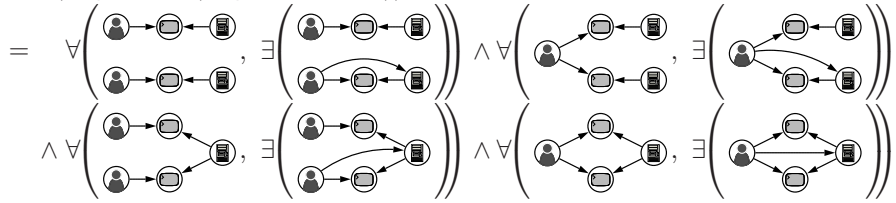
Wlp(`Login`, *secure*)
$= \mathrm{C}(\mathrm{Def}(\texttt{Login}) \Rightarrow \mathrm{L}(\texttt{Login}, \mathrm{A}(\texttt{Login}, \textit{secure})))$
$= \mathrm{C}((\mathrm{Appl}(\texttt{Login}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{Login}, \mathrm{A}(\texttt{Login}, \textit{secure})))$
$\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{Login}, \mathrm{A}(\texttt{Login}, \textit{secure})))$
$\equiv \mathrm{C}(\mathrm{L}(\texttt{Login}, \mathrm{A}(\texttt{Login}, \textit{secure})))$
$= \forall($ $, \mathrm{L}(\texttt{Login}, \mathrm{A}(\texttt{Login}, \textit{secure})))$
$\equiv$



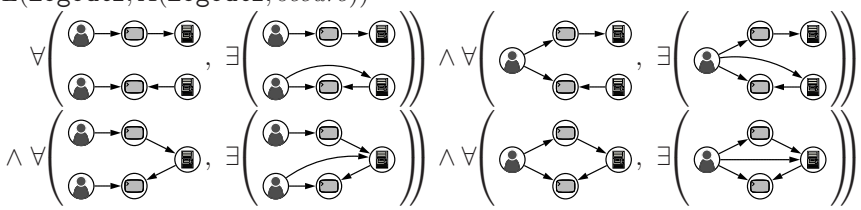
$\equiv$ *secure*

where we use Fact 5.(1)/(2) and 5.(4) for the last two equivalences, respectively (see Appendix C). For the program `Logout`, we have

L(`Logout1`, A(`Logout1`, *secure*))



$\mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \mathit{secure}))$

$=$ 

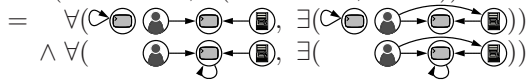
$\mathrm{Wlp}(\texttt{Logout}, \mathit{secure})$
$\mathrm{Wlp}(\{\texttt{Logout1}, \texttt{Logout2}\}, \mathit{secure})$
$= \mathrm{Wlp}(\texttt{Logout1}, \mathit{secure}) \wedge \mathrm{Wlp}(\texttt{Logout2}, \mathit{secure})$
$= \begin{array}{l} \mathrm{C}(\mathrm{Def}(\texttt{Logout1}) \Rightarrow \mathrm{L}(\texttt{Logout1}, \mathrm{A}(\texttt{Logout1}, \mathit{secure}))) \\ \wedge\ \mathrm{C}(\mathrm{Def}(\texttt{Logout2}) \Rightarrow \mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \mathit{secure}))) \end{array}$
if $\mathrm{C}(\mathrm{L}(\texttt{Logout1}, \mathrm{A}(\texttt{Logout1}, \mathit{secure}))) \wedge \mathrm{C}(\mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \mathit{secure})))$
if $\begin{array}{l} \forall(\text{  }),\ \mathrm{L}(\texttt{Logout1}, \mathrm{A}(\texttt{Logout1}, \mathit{secure}))) \\ \wedge\ \forall(\text{  }),\ \mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \mathit{secure}))) \end{array}$
if secure

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). For the program `ProcessLogin`, we show *secure* implies $\mathrm{Wlp}(\texttt{ProcessLogin}, \mathit{secure})$. Using Fact 4.(5), we assume here and show later, that for every subpogram P of `ProcessLogin`, *secure* implies $\mathrm{Wlp}(P, \mathit{secure})$.

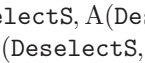
$\mathrm{Wlp}(\texttt{ProcessLogin}, \mathit{secure})$
$= \mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}; \texttt{LogS}{\downarrow}; \texttt{ClearLogS}{\downarrow}; \texttt{DeselectS}{\downarrow}, \mathit{secure})$
$= \mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}; \texttt{LogS}{\downarrow}; \texttt{ClearLogS}{\downarrow}, \mathrm{Wlp}(\texttt{DeselectS}{\downarrow}, \mathit{secure}))$
if $\mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}; \texttt{LogS}{\downarrow}; \texttt{ClearLogS}{\downarrow}, \mathit{secure})$
if $\mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}; \texttt{LogS}{\downarrow}, \mathrm{Wlp}(\texttt{ClearLogS}{\downarrow}, \mathit{secure}))$
if $\mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}; \texttt{LogS}{\downarrow}, \mathit{secure})$
if $\mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}, \mathrm{Wlp}(\texttt{LogS}{\downarrow}, \mathit{secure}))$
if $\mathrm{Wlp}(\texttt{SelectS}; \texttt{AccessS}{\downarrow}, \mathit{secure})$
if $\mathrm{Wlp}(\texttt{SelectS}, \mathrm{Wlp}(\texttt{AccessS}{\downarrow}, \mathit{secure}))$
if $\mathrm{Wlp}(\texttt{SelectS}, \mathit{secure})$
if secure

To prove the statement *secure* implies $\mathrm{Wlp}(\texttt{DeselectS}{\downarrow}, \mathit{secure})$, we show *secure* implies $\mathrm{Wlp}(\texttt{DeselectS}, \mathit{secure})$ (see Lemma 2, Appendix C).

$\mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure}))$

$=$ 

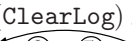
$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{DeselectS}, \mathit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{DeselectS}) \Rightarrow \mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{DeselectS}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure})))\\
&= \forall(\ \ ,\ \mathrm{L}(\texttt{DeselectS}, \mathrm{A}(\texttt{DeselectS}, \mathit{secure})))\\
&\text{if } \mathit{secure}
\end{aligned}
$$



where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). To prove the statement *secure* implies $\mathrm{Wlp}(\texttt{ClearLogS}\downarrow, \mathit{secure})$, we observe *secure* implies $\mathrm{Wlp}(\texttt{ClearLogS}, \mathit{secure})$ (see Lemma 2, Appendix C) even without the additional application condition:

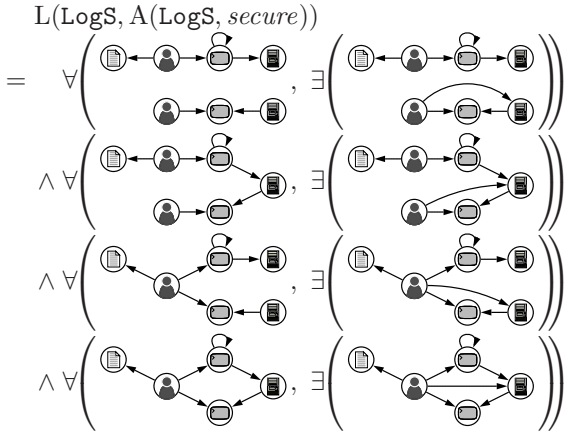
$$
\begin{aligned}
&\mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure}))\\
&= \mathrm{L}(\texttt{ClearLog}, \mathrm{A}(\texttt{ClearLog}, \mathit{secure}))\\
&= \quad \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))
\end{aligned}
$$

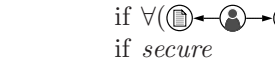
$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{ClearLogS}, \mathit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{ClearLogS}) \Rightarrow \mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{ClearLog}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\exists(\ \ ) \Rightarrow \mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure})))\\
&\text{if } \mathrm{C}(\mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure})))\\
&\text{if } \forall(\ \ ,\ \mathrm{L}(\texttt{ClearLogS}, \mathrm{A}(\texttt{ClearLogS}, \mathit{secure})))\\
&\text{if } \mathit{secure}
\end{aligned}
$$



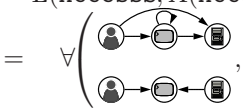
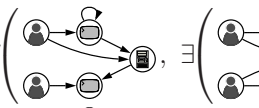
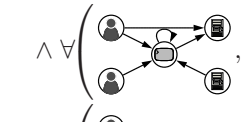
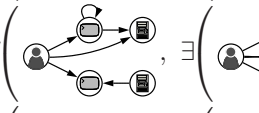
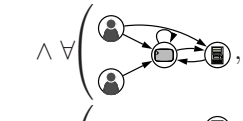
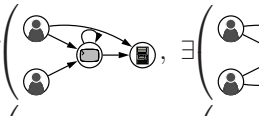
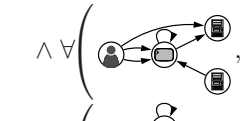
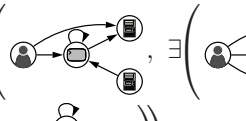
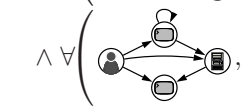
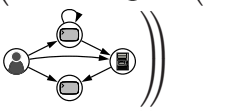
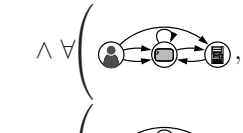
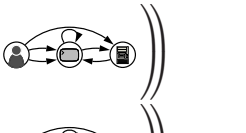
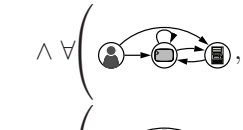
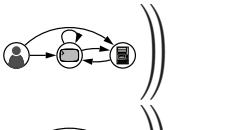
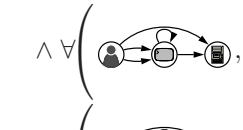
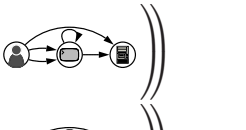
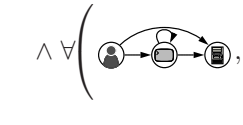
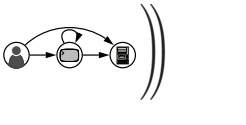
where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). For *secure* implies $\mathrm{Wlp}(\texttt{LogS}\downarrow, \mathit{secure})$, we show *secure* implies $\mathrm{Wlp}(\texttt{LogS}, \mathit{secure})$ (see Lemma 2, Appendix C):

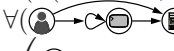
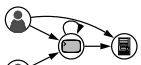
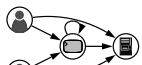
$$
\begin{aligned}
&\mathrm{L}(\texttt{LogS}, \mathrm{A}(\texttt{LogS}, \mathit{secure}))\\
&= \quad \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))
\end{aligned}
$$



$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{LogS}, \textit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{LogS}) \Rightarrow \mathrm{L}(\texttt{LogS}, \mathrm{A}(\texttt{LogS}, \textit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{LogS}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{LogS}, \mathrm{A}(\texttt{LogS}, \textit{secure})))\\
&\text{if } \mathrm{C}(\mathrm{L}(\texttt{LogS}, \mathrm{A}(\texttt{LogS}, \textit{secure})))\\
&\text{if } \forall(\text{  }),\ \mathrm{L}(\texttt{LogS}, \mathrm{A}(\texttt{LogS}, \textit{secure})))\\
&\text{if } \textit{secure}
\end{aligned}
$$

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). For the program `AccessS`, *secure* implies Wlp(`AccessS`, *secure*) seems obvious. However, *secure* alone is not invariant as the following calculation shows:

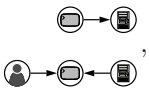
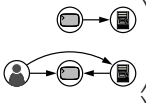
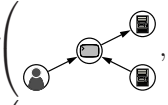
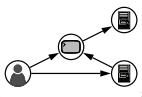
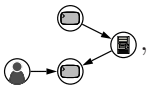
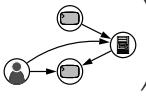
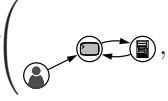
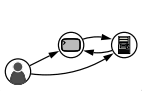
$$
\begin{aligned}
&\mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \textit{secure}))\\
= \quad &\forall\Big(\text{  }\Big) \wedge \forall\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \wedge \forall\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \wedge \forall\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \wedge \forall\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \vee \exists\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \vee \exists\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \vee \exists\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \vee \exists\Big(\text{  }\Big)\\
\wedge\ &\forall\Big(\text{  }\Big) \vee \exists\Big(\text{  }\Big)
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{AccessS}, \mathit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{AccessS}) \Rightarrow \mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \mathit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{AccessS}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \mathit{secure})))\\
&= \forall(\,\text{  }\,,\ \mathrm{L}(\texttt{AccessS}, \mathrm{A}(\texttt{AccessS}, \mathit{secure})))\\
&\text{if } \forall\Big(\text{  }\,,\ \exists\Big(\text{  }\Big)\Big) \wedge \mathit{secure}\\
&\text{if } \mathit{nosharedsessions} \wedge \mathit{secure}
\end{aligned}
$$

where

$$\mathit{nosharedsessions} = \neg\exists(\text{  })$$

and we use Fact 5.(1), 5.(2) and 5.(4) for the second last step (see Appendix C). This is a surprising result, as the condition *secure* needs to be strenghtened with the condition *nosharedsessions* to become invariant. This can be seen as follows: If a user "shares" a proposed session with another user, then he must also have an access right to the system. However, unless the access control starts in a state that already violates *nosharedsessions*, such a situation cannot occur within executions of `Control` as each new session is associated to exactly one user. For the program `SelectS`, we observe *secure* implies Wlp(`SelectS`, *secure*):

$$
\begin{aligned}
&\mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure}))\\
= \quad &\forall\Big(\text{  }\,,\ \exists\Big(\text{  }\Big)\Big) \wedge \forall\Big(\text{  }\,,\ \exists\Big(\text{  }\Big)\Big)\\
&\wedge \forall\Big(\text{  }\,,\ \exists\Big(\text{  }\Big)\Big) \wedge \forall\Big(\text{  }\,,\ \exists\Big(\text{  }\Big)\Big)
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{SelectS}, \mathit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{SelectS}) \Rightarrow \mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{SelectS}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure})))\\
&\equiv \mathrm{C}(\mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure})))\\
&= \forall(\,\text{  }\,,\ \mathrm{L}(\texttt{SelectS}, \mathrm{A}(\texttt{SelectS}, \mathit{secure})))\\
&\text{if } \mathit{secure}
\end{aligned}
$$

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). For the program `Revoke`, one can show that `LogoutUS`$\downarrow$ leaves no sessions for any selected user and system (see property (4)). As a consequence, `RevokeUS` will preserve the satisfaction of *secure*, as do all other parts of `Revoke`, hence *secure* implies Wlp(`Revoke`, *secure*).

(4) After execution of `LogoutUS`$\downarrow$, there is no established session left for any selected user and system: wlp(`LogoutUS`$\downarrow$, *noestablishedUS*) $\equiv$ true, where

$$\mathit{noestablishedUS} = \neg\exists(\text{  })$$

(5) C(Appl(`Logout1`)) ∧ C(Appl(`Logout2`)) is invariant for all programs P in `Control`, and all subprograms and rules of `Revoke` and `DeleteUser`.

Property (5) expresses that certain edges adjacent to a session node do not exist, while others have a multiplicity of at most 1. By using property (5), we can show Wlp(`LogoutUS`, false) implies *noestablishedUS* and thus show property (4):

$$
\begin{aligned}
&\text{Wlp}(\texttt{LogoutUS}, \text{false}) \Rightarrow \textit{noestablishedUS}\\
&= \text{Wlp}(\{\texttt{LogoutUS1}, \texttt{LogoutUS2}\}, \text{false}) \Rightarrow \textit{noestablishedUS}\\
&= (\text{Wlp}(\texttt{LogoutUS1}, \text{false}) \wedge \text{Wlp}(\texttt{LogoutUS2}, \text{false})) \Rightarrow \textit{noestablishedUS}\\
&= (\text{C}(\neg\text{Def}(\texttt{LogoutUS1})) \wedge \text{C}(\neg\text{Def}(\texttt{LogoutUS2}))) \Rightarrow \textit{noestablishedUS}\\
&\equiv \left(\begin{array}{l} \text{C}(\neg(\text{Appl}(\texttt{Logout1}) \wedge \exists(\text{⟳👤→▭←▤⟲}))) \\ \wedge\ \text{C}(\neg(\text{Appl}(\texttt{Logout2}) \wedge \exists(\text{⟳👤→▭→▤⟲})))\end{array}\right) \Rightarrow \textit{noestablishedUS}\\
&\overset{(5)}{\equiv} (\text{C}(\neg\exists(\text{⟳👤→▭←▤⟲})) \wedge \text{C}(\neg\exists(\text{⟳👤→▭→▤⟲}))) \Rightarrow \textit{noestablishedUS}\\
&\equiv \left(\begin{array}{l} \forall(\text{👤→▭←▤}, \neg\exists(\text{⟳👤→▭←▤⟲})) \\ \wedge\ \forall(\text{👤→▭→▤}, \neg\exists(\text{⟳👤→▭→▤⟲}))\end{array}\right) \Rightarrow \textit{noestablishedUS}\\
&\equiv (\textit{noestablishedUS} \wedge \neg\exists(\text{⟳👤→▭→▤⟲})) \Rightarrow \textit{noestablishedUS}\\
&\equiv \text{true}
\end{aligned}
$$

With the above statement, wlp(`LogoutUS`↓, *noestablishedUS*) ≡ wlp(`LogoutUS`*, Wlp(`LogoutUS`, false) ⇒ *noestablishedUS*) ≡ wlp(`LogoutUS`*, true) ≡ true.

Proving property (5) for all rules used in `Control` is tedious, but nonetheless straightforward, as every subcondition may handled separately. Intuitively only subprograms and rules have to be considered that contain a session node, and moreover, that create or delete edges adjacent to session nodes. Back to the proof *secure* implies `Revoke`, using Fact 4.(5), we assume here and show later, that for every subpogram P of `Revoke`, *secure* implies Wlp(P, *secure*).

$$
\begin{aligned}
&\text{Wlp}(\texttt{Revoke}, \textit{secure})\\
&= \text{Wlp}(\texttt{SelectUS}; \texttt{LogoutUS}\downarrow; \texttt{RevokeUS}; \texttt{DeselectUS}, \textit{secure})\\
&= \text{Wlp}(\texttt{SelectUS}; \texttt{LogoutUS}\downarrow; \texttt{RevokeUS}, \text{Wlp}(\texttt{DeselectUS}, \textit{secure}))\\
&\text{if } \text{Wlp}(\texttt{SelectUS}; \texttt{LogoutUS}\downarrow; \texttt{RevokeUS}, \textit{secure})\\
&\text{if } \text{Wlp}(\texttt{SelectUS}; \texttt{LogoutUS}\downarrow, \text{Wlp}(\texttt{RevokeUS}, \textit{secure}))\\
&\text{if } \text{Wlp}(\texttt{SelectUS}; \texttt{LogoutUS}\downarrow, \textit{secure})\\
&\text{if } \text{Wlp}(\texttt{SelectUS}, \text{Wlp}(\texttt{LogoutUS}\downarrow, \textit{secure}))\\
&\text{if } \text{Wlp}(\texttt{SelectUS}, \textit{secure})\\
&\text{if } \textit{secure}
\end{aligned}
$$

We prove the statement *secure* implies Wlp(`DeselectUS`, *secure*):

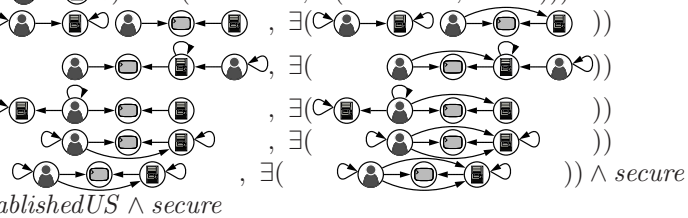
$$
\begin{aligned}
&\text{L}(\texttt{DeselectUS}, \text{A}(\texttt{DeselectUS}, \textit{secure}))\\
= \quad &\forall(\text{⟲👤👤→▭←▤⟳▤}, \exists(\text{⟲👤👤→▭←▤⟳▤}))\\
\wedge\ &\forall(\text{⟲👤👤→▭←▤⟲}\ \ , \exists(\text{⟲👤👤→▭←▤⟲}\ \ ))\\
\wedge\ &\forall(\ \ \text{⟳👤→▭←▤⟳▤}, \exists(\ \ \text{⟳👤→▭←▤⟳▤}))\\
\wedge\ &\forall(\ \ \text{⟳👤→▭←▤⟲}\ \ , \exists(\ \ \text{⟳👤→▭←▤⟲}\ \ ))
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{DeselectUS}, \textit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{DeselectUS}) \Rightarrow \mathrm{L}(\texttt{DeselectUS}, \mathrm{A}(\texttt{DeselectUS}, \textit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{DeselectUS}) \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{DeselectUS}, \mathrm{A}(\texttt{DeselectUS}, \textit{secure})))\\
&\equiv \mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{DeselectUS}, \mathrm{A}(\texttt{DeselectUS}, \textit{secure})))\\
&\equiv \mathrm{C}(\mathrm{L}(\texttt{DeselectUS}, \mathrm{A}(\texttt{DeselectUS}, \textit{secure})))\\
&\equiv \forall(\ \ ,\ \mathrm{L}(\texttt{DeselectUS}, \mathrm{A}(\texttt{DeselectUS}, \textit{secure})))\\
&\text{if } \textit{secure}
\end{aligned}
$$

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). We prove the statement *secure* implies Wlp(`RevokeUS`, *secure*):

$$
\begin{aligned}
&\mathrm{L}(\texttt{RevokeUS}, \mathrm{A}(\texttt{RevokeUS}, \textit{secure}))\\
&= \mathrm{L}(\texttt{Revoke}, \mathrm{A}(\texttt{Revoke}, \textit{secure}))\\
&= \quad \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{RevokeUS}, \textit{secure})\\
&= \mathrm{C}(\mathrm{Def}(\texttt{RevokeUS}) \Rightarrow \mathrm{L}(\texttt{RevokeUS}, \mathrm{A}(\texttt{RevokeUS}, \textit{secure})))\\
&= \mathrm{C}((\mathrm{Appl}(\texttt{RevokeUS}) \wedge \exists(\ \ )) \Rightarrow \mathrm{L}(\texttt{RevokeUS}, \mathrm{A}(\texttt{RevokeUS}, \textit{secure})))\\
&\equiv \mathrm{C}(\exists(\ \ ) \Rightarrow \mathrm{L}(\texttt{RevokeUS}, \mathrm{A}(\texttt{RevokeUS}, \textit{secure})))\\
&\equiv \quad \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\quad \wedge \forall(\ \ ,\ \exists(\ \ ))\\
&\text{if } \forall(\ \ ,\ \exists(\ \ )) \wedge \textit{secure}\\
&\text{if } \textit{noestablishedUS} \wedge \textit{secure}
\end{aligned}
$$

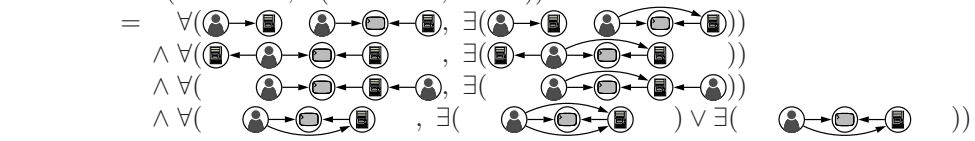


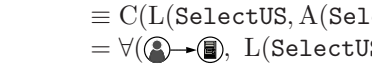
where we use Fact 5.(1), 5.(2) for the second and 5.(4) for the third last step (see Appendix C). For *secure* implies Wlp(`LogoutUS`$\downarrow$, *secure*), we have to show *secure* implies Wlp(`LogoutUS`, *secure*) (see Lemma 2, Appendix C). The proof is similar to the one for `Logout`:

$$
\begin{aligned}
&\mathrm{L}(\texttt{LogoutUS1}, \mathrm{A}(\texttt{LogoutUS1}, \textit{secure})) = \mathrm{L}(\texttt{Logout1}, \mathrm{A}(\texttt{Logout1}, \textit{secure}))\\
&\mathrm{L}(\texttt{LogoutUS2}, \mathrm{A}(\texttt{LogoutUS2}, \textit{secure})) = \mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \textit{secure}))
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Wlp}(\texttt{LogoutUS}, \textit{secure})\\
&= \mathrm{Wlp}(\texttt{LogoutUS1}, \textit{secure}) \wedge \mathrm{Wlp}(\texttt{LogoutUS2}, \textit{secure})\\
&= \quad \mathrm{C}(\mathrm{Def}(\texttt{LogoutUS1}) \Rightarrow \mathrm{L}(\texttt{LogoutUS1}, \mathrm{A}(\texttt{LogoutUS1}, \textit{secure})))\\
&\quad \wedge \mathrm{C}(\mathrm{Def}(\texttt{LogoutUS2}) \Rightarrow \mathrm{L}(\texttt{LogoutUS2}, \mathrm{A}(\texttt{LogoutUS2}, \textit{secure})))\\
&\text{if} \quad \mathrm{C}(\mathrm{L}(\texttt{LogoutUS1}, \mathrm{A}(\texttt{LogoutUS1}, \textit{secure})))\\
&\quad \wedge \mathrm{C}(\mathrm{L}(\texttt{LogoutUS2}, \mathrm{A}(\texttt{LogoutUS2}, \textit{secure})))\\
&\text{if } \textit{secure}
\end{aligned}
$$

For the `SelectUS`, we observe *secure* implies Wlp(`SelectUS`, *secure*):

L(`SelectUS`, A(`SelectUS`, *secure*))
= 

Wlp(`SelectUS`, *secure*)
= C(Def(`SelectUS`) ⇒ L(`SelectUS`, A(`SelectUS`, *secure*)))
= C((Appl(`SelectUS`) ∧ true ∧ true) ⇒ L(`SelectUS`, A(`SelectUS`, *secure*)))
≡ C(true ⇒ L(`SelectUS`, A(`SelectUS`, *secure*)))
≡ C(L(`SelectUS`, A(`SelectUS`, *secure*)))
= 
if *secure*

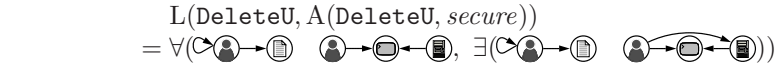
where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C).

For the program `DeleteUser`, one can show that `LogoutU`↓ leaves no sessions for any selected user (similar to property (4)). As a consequence, `RevokeU`↓ will preserve the satisfaction of *secure*, as do all other parts of `DeleteUser`, hence *secure* implies Wlp(`DeleteUser`, *secure*).

We show *secure* implies Wlp(`DeleteUser`, *secure*). Using Fact 4.(5), we assume here and show later, that for every subpogram P of `DeleteUser`, *secure* implies Wlp(P, *secure*).

Wlp(`DeleteUser`, *secure*)
= Wlp(`SelectU`; `LogoutU`↓; `RevokeU`↓; `ClearLogU`↓; `DeleteU`, *secure*)
= Wlp(`SelectU`; `LogoutU`↓; `RevokeU`↓; `ClearLogU`↓, Wlp(`DeleteU`, *secure*))
if Wlp(`SelectU`; `LogoutU`↓; `RevokeU`↓; `ClearLogU`↓, *secure*)
if Wlp(`SelectU`; `LogoutU`↓; `RevokeU`↓, Wlp(`ClearLogU`↓, *secure*))
if Wlp(`SelectU`; `LogoutU`↓; `RevokeU`↓, *secure*)
if Wlp(`SelectU`; `LogoutU`↓, Wlp(`RevokeU`↓, *secure*))
if Wlp(`SelectU`; `LogoutU`↓, *secure*)
if Wlp(`SelectU`, Wlp(`LogoutU`↓, *secure*))
if Wlp(`SelectU`, *secure*)
if *secure*

We prove the statement *secure* implies Wlp(`DeleteU`, *secure*):

L(`DeleteU`, A(`DeleteU`, *secure*))
= 

Wlp(`DeleteU`, *secure*)
= C(Def(`DeleteU`) ⇒ L(`DeleteU`, A(`DeleteU`, *secure*)))
= C((Appl(`DeleteU`) ∧ true ∧ true) ⇒ L(`DeleteU`, A(`DeleteU`, *secure*)))
if C(L(`DeleteU`, A(`DeleteU`, *secure*)))
if 
if *secure*

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C). For *secure* implies Wlp(`ClearLogU`↓, *secure*), we have to show *secure* implies Wlp(`ClearLogU`, *secure*) (see Lemma 2, Appendix C). The proof is similar to the one for `ClearLogS`:

$$\mathrm{L}(\texttt{ClearLogU}, \mathrm{A}(\texttt{ClearLogU}, \mathit{secure})) = \mathrm{L}(\texttt{ClearLog}, \mathrm{A}(\texttt{ClearLog}, \mathit{secure}))$$

$$\begin{aligned}
&\mathrm{Wlp}(\texttt{ClearLogU}, \mathit{secure}) \\
=\ &\mathrm{C}(\mathrm{Def}(\texttt{ClearLogU}) \Rightarrow \mathrm{L}(\texttt{ClearLogU}, \mathrm{A}(\texttt{ClearLogU}, \mathit{secure}))) \\
\text{if}\ &\mathrm{C}(\mathrm{L}(\texttt{ClearLogU}, \mathrm{A}(\texttt{ClearLogU}, \mathit{secure}))) \\
\text{if}\ &\mathit{secure}
\end{aligned}$$

To prove *secure* implies Wlp(`RevokeU`↓, *secure*), we have to show *secure* implies Wlp(`RevokeU`, *secure*) (see Lemma 2, Appendix C). The proof is similar to the one for `RevokeUS` and obmitted. For *secure* implies Wlp(`LogoutU`↓, *secure*), we have to show *secure* implies Wlp(`LogoutU`, *secure*) (see Lemma 2, Appendix C). The proof is similar to the one for `Logout`:

$$\begin{aligned}
&\mathrm{L}(\texttt{LogoutU1}, \mathrm{A}(\texttt{LogoutU1}, \mathit{secure})) = \mathrm{L}(\texttt{Logout1}, \mathrm{A}(\texttt{Logout1}, \mathit{secure})) \\
&\mathrm{L}(\texttt{LogoutU2}, \mathrm{A}(\texttt{LogoutU2}, \mathit{secure})) = \mathrm{L}(\texttt{Logout2}, \mathrm{A}(\texttt{Logout2}, \mathit{secure}))
\end{aligned}$$

$$\begin{aligned}
&\mathrm{Wlp}(\texttt{LogoutU}, \mathit{secure}) \\
=\ &\mathrm{Wlp}(\texttt{LogoutU1}, \mathit{secure}) \wedge \mathrm{Wlp}(\texttt{LogoutU2}, \mathit{secure}) \\
=\ &\quad \mathrm{C}(\mathrm{Def}(\texttt{LogoutU1}) \Rightarrow \mathrm{L}(\texttt{LogoutU1}, \mathrm{A}(\texttt{LogoutU1}, \mathit{secure}))) \\
&\wedge\ \mathrm{C}(\mathrm{Def}(\texttt{LogoutU2}) \Rightarrow \mathrm{L}(\texttt{LogoutU2}, \mathrm{A}(\texttt{LogoutU2}, \mathit{secure}))) \\
\text{if}\ &\quad \mathrm{C}(\mathrm{L}(\texttt{LogoutU1}, \mathrm{A}(\texttt{LogoutU1}, \mathit{secure}))) \\
&\wedge\ \mathrm{C}(\mathrm{L}(\texttt{LogoutU2}, \mathrm{A}(\texttt{LogoutU2}, \mathit{secure}))) \\
\text{if}\ &\mathit{secure}
\end{aligned}$$

For the `SelectU`, we observe *secure* implies Wlp(`SelectU`, *secure*):

$$\begin{aligned}
&\mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure})) \\
=\ &\quad \forall(\ \ \exists(\ \ ))\ \wedge\ \forall(\ \ \exists(\ \ ))
\end{aligned}$$

$$\begin{aligned}
&\mathrm{Wlp}(\texttt{SelectU}, \mathit{secure}) \\
=\ &\mathrm{C}(\mathrm{Def}(\texttt{SelectU}) \Rightarrow \mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure}))) \\
=\ &\mathrm{C}((\mathrm{Appl}(\texttt{SelectU}) \wedge \mathrm{true} \wedge \mathrm{true}) \Rightarrow \mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure}))) \\
\equiv\ &\mathrm{C}(\mathrm{true} \Rightarrow \mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure}))) \\
\equiv\ &\mathrm{C}(\mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure}))) \\
=\ &\forall(\ ),\ \mathrm{L}(\texttt{SelectU}, \mathrm{A}(\texttt{SelectU}, \mathit{secure}))) \\
\equiv\ &\mathit{secure}
\end{aligned}$$

where we use Fact 5.(1), 5.(2) and 5.(4) for the last step (see Appendix C).

Figure 5 summarizes the proofs given here, where "..." marks the parts that were not considered further. The conclusion is that most programs and rules preserve the satisfaction of *secure*. Noteworthy exceptions are `AccessS`, where one additionally has to ensure that there do not exist shared sessions, `RevokeUS`

and RevokeU, where the precondition *noestablishedUS* and *noestablishedU* are required, respectively, which can be only shown if Appl(Logout1) ∧ Appl(Logout2) is invariant. While tedious, the proof of the missing parts should be straightforward (only existential quantifications in the statements).

Figure 5. Structure of the proof